

**Positioning technology:  
Relevant Regulations of  
USA, Japan, Germany and Italy**

Report of the Support Project of NAVI-programme: Regulatory Framework



Report of the NAVI Regulatory Framework -project

**Positioning technology: Relevant Regulations of  
USA, Japan, Germany and Italy**

Raija Tervo-Pellikka

Samuli Simojoki

**Publisher:**

Helsinki Institute for Information Technology (HIIT)  
Tammasaarekatu 3  
P.O. box 9800  
FIN 02015 HUT, Finland  
info@hiit.fi  
samuli.simojoki@hiit.fi

Helsinki Institute for Information Technology (HIIT) is a joint research unit of the two leading research universities in Helsinki, Finland, the University of Helsinki (UH) and the Helsinki University of Technology (HUT).

<b>1. Background of the Report .....</b>	<b>1</b>
<b>2. Introduction to Positioning Technology and its Regulation.....</b>	<b>3</b>
2.1. <i>What is positioning technology and how is it utilised?</i> .....	3
2.2. <i>Positioning Technology: Legal Perspective</i> .....	4
2.3. <i>Scope of this Report</i> .....	4
2.4. <i>Classifications and Concepts</i> .....	5
<b>3. Situation in USA .....</b>	<b>6</b>
3.1. <i>Privacy Regulations in USA in General</i> .....	6
3.2. <i>Actors Involved in Privacy Debate</i> .....	7
3.3. <i>Overview of Online Privacy in the USA</i> .....	8
3.4. <i>Applicable Regulations in the Telecommunications Sector</i> .....	9
3.5. <i>Utilisation of Customer Proprietary Network Information</i> .....	9
3.6. <i>Initiative Concerning Location Information</i> .....	12
3.7. <i>E911 and Positioning</i> .....	13
3.8. <i>Conclusion</i> .....	15
<b>4. Situation in Japan.....</b>	<b>16</b>
4.1. <i>Data protection regulatory framework overview</i> .....	16
4.2. <i>Overview of the positioning technology and services utilised</i> .....	17
4.3. <i>Regulatory bodies for the data protection in the telecommunications field</i> .....	17
4.4. <i>Data protection regulations for telecommunications and position technology</i> .....	18
4.5. <i>Other related legislation</i> .....	21
4.6. <i>Summary of the data protection principles</i> .....	22
4.7. <i>Discussion and views</i> .....	23
<b>5. Situation in Italy .....</b>	<b>25</b>
5.1. <i>Data protection regulatory framework overview</i> .....	25
5.2. <i>Positioning technology and services overview</i> .....	25
5.3. <i>Regulatory bodies for the data protection in the telecommunications field</i> .....	26
5.4. <i>Data protection regulations for telecommunications and position technology</i> .....	27
5.5. <i>Discussion and views</i> .....	30
<b>6. Situation in Germany.....</b>	<b>32</b>
6.1. <i>Data Protection in Germany - An Introductory Overview</i> .....	32
6.2. <i>Regulatory bodies for the data protection in the telecommunications field</i> .....	32
6.3. <i>Data protection regulations for telecommunications and position technology</i> .....	33
6.4. <i>Supervisory authorities – data protection ombudsman of enterprises</i> .....	35
6.5. <i>Data Protection Legislation in Telecommunication Sector</i> .....	36

## Appendices

Appendix 1: References For the Report Concerning USA

Appendix 2: References For the Report Concerning Japan

Appendix 3: Extract From Fcc Documentation Concerning E911 Timetable

Appendix 4: FCC Rules For The Use Of The Customer Proprietary Network Information

Appendix 5: References for the Report related Concerning Italy

## **Positioning technology: Relevant Regulations of USA, Japan, Germany and Italy**

### **Report of the Support Project of NAVI-programme: Regulatory Framework**

#### ***1. Background of the Report***

Personal Navigation (NAVI) programme was launched in May 2000 by the Ministry of Transport and Communications in Finland. NAVI is a research and development as well as co-operation programme and it will last three years (2000–2002). The programme includes research, product and service development, regulation, awareness activities, education, follow-up, co-ordination and strategy work. The aim of the programme is to develop and test infrastructure, devices, software and services within the framework of consumer demand and the possibilities of technology.

The programme consists of the projects focusing on vertical applications, generic technologies, horizontal support projects, practical training and co-ordination. The seven identified vertical application areas are mobile work, transactions, shopping and delivery, hobbies and sports, tourism and culture, public transport, welfare and unfettered mobility as well as safety. The three support projects are 1) the regulatory framework, 2) usability and ethical audit 3) service architecture and meta data. The four areas of generic technology are map and route services, in-door positioning and guidance, location services and navigation devices.

This report pertains to the support project called Regulatory Framework. The goal of the project is to study and report on the regulation affecting the development, provision and utilisation of positioning technology -based services. The following reports will be prepared in the project:

- (i) Current Regulatory Framework

In this report the regulatory framework in force in Finland and in the European Union is explored. Firstly, the relevant regulation is identified and interpreted in the light of the positioning technology. In this report the focus is on the current regulatory framework.

(ii) The impact of the regulatory environment on services and business models based on utilisation of positioning technology

In this report the current and anticipated regulatory framework is analysed in light of its impact on the services based on positioning technology and business models related to them.

(iii) Development of the regulation from the point of view of fundamental data protection principles.

In this report the information gathered in the project is used in order to assess the location-based services and their regulations from the point of view of fundamental data protection principles. The purpose of the report is to seek practises and regulations that would reflect the goals and principles and the data protection principles.

(iv) Intellectual property issues related to utilisation of location data and spatial data.

Intellectual property rights related to spatial data are an important aspect of regulation. A separate report shall be drafted on these issues.

(v) The relevant regulation of USA, Japan and other countries

The services developed by the companies within the NAVI-programme are directed to the international markets. Therefore the scope of the support project is essentially international, and the regulative frameworks of other relevant markets need also to be analysed.

Even though the assessment of the EU legislation provides general framework of the legislation in EU member states, a more detailed analysis of the domestic legislation in certain key market areas is necessary even within the European Union.

Also the key market areas outside the European Union, such as United States and Japan, will be analysed.

(v) Guidebook to regulatory framework of positioning technology

In this guidebook a brief and easy-to-read overview of the regulatory framework is provided.

It is possible that the steering group of the project will decide on changes to the aforementioned list.

This is the first version of the report “Current Regulatory Framework”. Preparation of the report is a continuous process, and not all regulative areas are covered in this first version of the report. The report will be updated at least semi-annually to correspond to the then-current legislative situation.

It is underlined that the report does not as such intend to be jurisprudential academic research paper but rather a practise-oriented report directed to serve the practical need of the companies and other interest groups within the Navi-programme.

## ***2. Introduction to Positioning Technology and its Regulation***

### **2.1. What is positioning technology and how is it utilised?**

There are a wide variety of different positioning technologies available. In general, the most relevant technologies for this report are satellite-based positioning (i.e. GPS), and positioning based on mobile phone base stations. There exists also other positioning technologies methods,

but the regulatory questions related to those technologies do not usually differ from the aforementioned technologies.

Positioning can be utilised in relation to a wide variety of services. The services may help people to navigate on work-related and leisure journeys, to choose the route and mode of transport necessary to reach a particular destination, and to find the service or product that they desire. Often location-based services are ordinary content services where the delivered content is automatically customised with regard to the location of the user.

## **2.2. Positioning Technology: Legal Perspective**

In a very general level there are three main fields of interest that needs to be analysed. First, the knowledge on a location of a person is very sensitive information. Therefore data protection issues are of high importance when implementing location-based services. Second, when operating in the digital environment, intellectual property rights (IPR) become complicated. Among the IPR-related issues that need clarification are IPR-nature of location data and spatial data as well as issues related to licensing and utilisation of the content used in provision of the location-based services. Third, commercial utilisation presupposes reliable and effective contractual practise. As the mobile environment is a difficult forum for concluding agreements, and as the new EU legislation is setting forth new requirements for the agreements concluded over communication networks, the relevant contract law will be analysed. Fourth, liability questions pertaining to the location-based services need to be analysed. Finally, regulative issues in certain important fields, such as direct marketing and employment relations, are analysed.

## **2.3. Scope of this Report**

In the Current Regulatory Framework -report prepared by the project, it has been concluded that data protection regulations are the most important field of regulation with respect to provision of location-based services. This entails to the fact that data protection regulations are likely to affect the nature of the location-based services and the nature these services are technically constructed, marketed and agreed on. Furthermore, in the field of data protection there

is potentially service-specific regulations for to location-based services. In spite of international treaties and organisation in the field, data protection regulations are heavily affected by national legal cultures and historical and political interests. Thus, there is considerable difference even with regard to the main principles of data protection under different legislations.

There are certainly substantial differences with regard to, for example contractual and liability law in different legislations, but these regulations are not specific to the location-based services. With regard to intellectual property issues, it can be concluded, that even though substantial national differences exist (for example the nature and extent of database protection and the protection of collections of information), the main fields of intellectual property, such as copyright, are based on international treaties.

For the above-mentioned reasons the analysis of this report is mainly limited to the analysis of data protection issues in the selected countries, and contractual, liability and intellectual property rights issues are not discussed.

#### **2.4. Classifications and Concepts**

In this report classifications and concepts developed in the Regulatory Framework –report and in the vocabulary-working group (sanastotyöryhmä) of the Navi Programme has been utilised.

### **3. Situation in USA**

#### **3.1. Privacy Regulations in USA in General**

Generally speaking there is no general data protection regulation in force in the USA. Instead, privacy rights have developed in the form of industry-specific statutes as well as in the form of self-regulation regimes.

In spite of the lack of general data protection law, the US Constitution is interpreted so as to guarantee a certain kind of a right to privacy. This constitutional right protects the privacy of individuals to some extent even in the absence of express regulations. While the U.S. Constitution does not explicitly use the word "privacy," several of its provisions protect its different aspects. The strongest protections arise from the Fourth Amendment, which safeguards individuals in their persons, homes, papers, and effects, from unreasonable searches and seizures. The Supreme Court first declared that citizens have a "reasonable" and "legitimate" expectation of privacy in their communications as central part of the Fourth Amendment in a landmark case *Katz v. United States* in 1967. In the 1960s and 1970s, the Supreme Court defined the concept of privacy to include personal decisions concerning reproduction, sex, and marriage. In *Whalen v. Roe* (1977), the Supreme Court held that the Fourteenth Amendment protects the privacy of certain information, in that case, sensitive prescription drug data collected by the state. As can be seen, the privacy discussions in the USA have developed recently.

Earlier the USA approach to privacy has mainly been concerned with the relationships between an individual and the state.

The European concept of privacy as the right of individuals to control information about themselves is not as widely applicable as in Europe. However, there is a variety of industry-specific legislation designed to protect the right to privacy, including the Electronic Communications Privacy Act, the Telephone Consumer Protection Act, the Health Insurance Portability and Accountability Act and Children's Online Privacy Protection Act. Recent regulation concerning utilisation of health information has had substantial influence for the industry forcing development of the information systems and practises.

Federal legislator is not solely competent in the field of privacy issues, but privacy regulations exist widely also in the state level, making the regulative environment somewhat complex. There is diverse legislation in different fields of business, especially in certain fields as banking and consumer protection. Thus, in order to ensure compliance with all applicable federal and state regulations, local counsel should be sought before implementing location-based services in the USA.

### **3.2. Actors Involved in Privacy Debate**

#### FCC

Federal Communications Commission (FCC) is an independent governmental organisation, directly responsible to the US Congress. Among its wide responsibilities are regulating interstate and international communications by radio, television, wire, satellite and cable. Thus FCC supervises, among other things, the provision of mobile telecommunications services. FCC has in certain cases a right to enact rules specifying the regulations set forth in federal legislation. As shall be seen later in this report, FCC has enacted regulations concerning privacy in the provision of telecommunications services.

#### FTC

Federal Trade Commission (FTC) is a governmental agency with a variety of responsibilities and mandates, one of them being the consumer protection. As part of its role in the field of consumer protection, FTC, among other things, monitors information and practises of companies trying to ensure that companies are not making misrepresentations.

#### Interest Groups

There are several interest groups active in the field of privacy and telecommunications issues, most important of them probably being the Cellular Telecommunications & Internet Associa-

tion (CTIA). Among the privacy advocates, active groups include Electronic Privacy Information Center (EPIC) and American Civil Liberties Union (ACLU).

### Industry Views for Privacy

In general the approach towards privacy in the USA has always favoured self-regulatory approach. This has been evident also in the public discussions regarding privacy. The industry has usually preferred self-regulatory approach, where companies may adopt their own privacy policies enforced by FTC instead of detailed rules enforced by authorities.

However, as will be explained in the next Section, CTIA and many other industry groups have proposed and favoured FCC rule-making for location data. There are several reasons for this, one of them being the building of consumer confidence for location-based services.

### **3.3. Overview of Online Privacy in the USA**

As there is no general data protection regulations in force, generally speaking, in the absence of industry-specific regulations (whether federal or state), a company is free to process personal data without limitations, provided that the somewhat limited Constitutional right to privacy is not limited.

However, in case a company has published a privacy policy, it must adhere to such policy. In protecting consumers' interests and protecting consumers from misrepresentations given by companies, FTC has adopted an active role in the online privacy legislation enforcing self-regulatory policies adopted by companies. The Federal Trade Commission (FTC) has taken the approach that a company must abide to the privacy policy it has published. Non-compliance with the published privacy rules is a misrepresentation, and FTC has extensive enforcement powers to act against companies giving misrepresentations to consumers. A company that knowingly is in breach of its privacy policy risks, among other things, facing punitive damages. Thus, companies publishing privacy policies should ensure compliance with such policies. Indeed, FTC has in some cases taken rigorous measures against companies not in compliance with their privacy policy.

There is one major federal on-line privacy law in force, Children's Online Privacy Protection Act (COPPA), which generally speaking prohibits on-line collection of personal data of children without express prior consent of the parents by websites or online services directed to children. As the act expressly covers both websites and online services, the law could have implications also for the providers of location-based services, and special care should be taken before implementing location-based services directed for children. Interpretation of whether a website or online service is directed to children depends in practice on an overall judgement, although FTC has published regulations specifying the principles of interpretation. The principles of the COPPA reflect those of European privacy principles: the necessity principle and the principle of exclusivity of purpose can both be found in the COPPA.

Outside the telecommunications regulations the privacy regulations in the US are diverse and complex. As mentioned, there is no general privacy regulation, but there are several regulations for specific industries and services (such as health care). Such regulations are often very detailed and complex. Furthermore, many States have adopted their own regulations so that the compliance with the federal regulations is not always sufficient.

### **3.4. Applicable Regulations in the Telecommunications Sector**

In general it can be concluded that the regulative situation in the USA with regard to privacy issues related to wireless telecommunications is under active discussion and development. There are three major issues that have been discussed lately, one being regulations concerning Customer Proprietary Network Information (CPNI), another utilisation of location information contained in the CPNI, and third being e911 regulations. These issues will be introduced in the next chapters.

### **3.5. Utilisation of Customer Proprietary Network Information**

The Telecommunications Act of 1996 includes rather detailed provisions regarding the utilisation of Customer Proprietary Network Information ("CPNI"). Section 222 of the Act enacts statutory restrictions on the use of CPNI by telecommunications carriers. Section 222 restricts

both the disclosure of CPNI to third parties, as well as the manner in which a carrier may use CPNI for the provision and marketing of its own services. According to the section 222 "every telecommunications carrier has a duty to protect the confidentiality of proprietary information of . . . customers." A telecommunications carrier may "use, disclose or permit access to individually identifiable CPNI" only in providing "the telecommunications service from which such information is derived" or "services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories." Telecommunications carriers must obtain customer "approval" prior to using CPNI for any purposes other than those expressly permitted by § 222.

Section 222 was amended by the Wireless Communications and Public Safety Act of 1999. Among other things, Public Safety Act added subsection (f) to § 222, which provides as follows:

(f) Authority to use wireless location information.

For purposes of subsection (c)(1), without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to -

(1) call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d) of this title), other than in accordance with subsection (d)(4);

Federal Communications Commission (FCC) may enact rules that would clarify the Section 222. In February 1998 FCC enacted one set of rules (hereinafter "Rules I") to clarify the obligations under Section 222. In the Rules I the Commission ordered that in order to ensure the "informed consent" of consumers for use of their CPNI in a manner other than specifically allowed under section 222(c)(1), Teleoperators would be required to obtain express written, oral or electronic consent from their customers, i.e., a all-embracing "opt in" requirement, before a carrier could use CPNI to market services outside the customer's existing service relationship with that carrier. The Commission also concluded that a Teleoperator must notify the customer of the customer's rights before soliciting approval to use the customer's CPNI.

FCC also adopted the so called the "total service approach" allowing carriers *and* their affiliates to use customers' CPNI, without notice or approval, to market services within the package of services to which the customer already subscribes to. This approach recognized that the customer may be fairly considered to have given implied consent to the carrier's use of CPNI within the total service package to which the customer subscribes.

In short it can be concluded that in some respects the Rules I corresponded to the European approach. There is some kind of a principle of exclusivity of purpose, one of the main principles of the European data protection regime, present in the regulations, limiting the utilisation of the information for certain purposes. The exclusivity of purpose –principle is not generally recognised in the USA. Within EU a Teleoperator is not allowed to utilise traffic data (as defined in the new TelePrivacy Directive) for marketing electronic communications services without user's consent, whereas in under the Rules I such marketing would be allowed.

Certain Teleoperators, being unsatisfied with Rules I, appealed to the court claiming the Rules I violating constitutional right to free speech. Without going into details of a complex legal argumentation, the court agreed with the Teleoperators, and found that the Rules I regulated protected commercial speech and thus violated the First Amendment. Specifically, the court found that the opt-in regime was not sufficiently narrowly tailored because FCC had failed to adequately consider an opt-out option. Grounds for this reasoning were in the principle that the Constitutional rights should be limited only as little as necessary for the legitimate purpose.

Recently, on 25 July 2002 FCC enacted a new set of rules taking into account the court's decision (hereinafter "Rules II, rules attached to this report). The Rules II include both opt-in and opt-out approach. For Teleoperators sharing information with affiliates that provide "communications-related" services, the FCC adopted the informed opt-out principle under which the Teleoperator must notify the customer of the disclosure of the information, and if the customer does not object, Teleoperator may share the information, and such affiliates may use the information. It should be noted that the definition of an affiliate is rather broad, covering Teleoperator's agents, affiliates, joint venture partners and independent contractors.

For affiliates that do not provide "communications-related" services and for unrelated third parties FCC ordered opt-in approach, under which the customer must grant its "affirmative, express consent" before usage, disclosure, or access to the requested CPNI is allowed. The Rules II include detailed provisions on the nature of the opt-in procedure and on the information to be provided before the disclosure or use of the information on the basis of the opt-out procedure.

Due to the recent implementation of the Rules II, their applicability has not been yet tested. However, it seems that the opt-in principle for direct marketing is the main rule under the rules, allowing opt-out only in the case of communications-related services, expressly including information services typically provided by telecommunications carriers. The contents of such information services has been further defined with a reference to the Communications Act of 1934, and with an express exclusion of retail consumer services such as travel reservation services or mortgage lending services. The detailed context of the term “communications-related services”, however, remains open to various interpretations.

### **3.6. Initiative Concerning Location Information**

The aforementioned Telecommunications Act 222 § covers also the utilisation of location information. The Cellular Telecommunications & Internet Association (“CTIA”) made on 22 November 2000 an initiative for a separate rule-making concerning utilisation of location information. CTIA argued utilisation of location information being such a separate and special field, that separate rules should be adopted in order to facilitate industry development and clarify the legal basis for location-based services.

Background for the initiative was partly CTIA’s dissatisfaction with the Rules I adopted by the FCC, and CTIA’s willingness to pursue the initiative was substantially weakened when the court ruled Rules I unconstitutional. However, in relation to this initiative a fruitful discussion regarding the utilisation of location data has taken place. The comments of different interest groups and companies can be found in the FCC web pages (docket 01-72 in the e-filing system). In the discussion most parties active in the field, including telecom companies, manufacturers of terminal and network equipment and privacy interest groups agreed with the CTIA on the need for more detailed and express regulations with regard to the utilisation of location information.

On 24 July 2002 FCC gave an order under which they denied CTIA’s request for rule-making. According to the Telecommunications Act 222 § Teleoperators are required to obtain a customer’s “express prior authorization” before using or disclosing wireless location information. FCC found that the requirement leaves no doubt that a customer must explicitly ar-

ticulate approval before a carrier can use that customer's location information. Further, the FCC indicated that it is "prepared to vigorously enforce the law as written," and that adopting rules at this point would not be appropriate, given the nascent state of wireless location based services.

In short, FCC stated that the requirement of "express prior authorization" in Section 222(f) of the Telecommunications Act is clear and unambiguous, and that wireless carriers must receive a customer's explicit approval before using their location information.

CTIA argued in its initiative that adopting separate rules would promote the acceptance of new location-based services by establishing a clear framework for industry to design the services and consumers to predict how their location information will be handled. FCC, found just the opposite to be more favourable for the development of the market, arguing that because of the nascent state of location-based services, FCC did not want to constrain technology or consumer choices via rules.

The wording of the order suggests, that FCC interprets the Section 222(f) not allowing any kind of implied consent for the use of location information. As concluded in the Regulatory Framework –report, under the Finnish and European regulations an implied consent might be accepted and used in certain situations, where the user is necessarily aware of the nature of the service requiring spatial data. However, opt-out regime is not allowed in neither of the regulations, the possible differences being in the interpretation of the opt-in principle.

### **3.7. E911 and Positioning**

Perhaps the most important regulation in the Wireless Communications and Public Safety Act of 1999 ("911 Act") was the introduction of 911 as the general nation-wide emergency number with the goal of being able to locate every emergency call made to that number. The Act will substantially affect, and has already affected, the operating environment of the telecom companies and of the providers of location-based services.

The implementation of emergency call location technology was divided into two steps: in phase I all Teleoperators were to be able to deliver the location of the cell site or base station receiving the 911 call, which provides only a rough indication of the caller's location. The deadline for implementing phase I has already passed, and by now all Teleoperators in USA should be able to deliver, at request, the location of the cell that has received the emergency call.

In phase II the Teleoperators are to be able to locate the emergency calls up to the precision of 50 or 100 meters. This entails technical changes either in the network equipment (in the case of network-based positioning) or in the handset of the user (in the case of satellite positioning such as GPS). As Teleoperators have adopted different technologies for the implementation of the phase II, handsets of different Teleoperators will not be compatible.

However, the technical implementation of the phase II has proven difficult, and the deadlines have been postponed several times. Generally there are three categories of dead-lines for different Teleoperators to fulfil the phase II requirements: (i) certain major nation-wide Teleoperators have proposed their own roll-out timetable, which FCC has accepted, (ii) FCC has ordered implementation deadlines for Teleoperators with more than 500.000 subscribers and (iii) for Teleoperators with less than 500.000 subscribers (See appendix).

FCC is determined to enforce these deadlines and has already by now fined Teleoperators that have been delayed in their implementation of the phase II. For example AT&T has received a multi-million dollar fine for not complying with the set timetable in the implementation of the emergency call location. The final goal of the FCC is, that by 31 December 2005 95 % of the mobile phones could be positioned with the required accuracy. FCC has expressed its commitment to hold on to this dead-line.

The e911 regulation seems to have several implications for the wireless markets: firstly, it has forced the development of location technology to proceed faster, secondly, it has diverged the mobile phone markets in the USA (into handsets with GPS-capability and handsets enabling network-based positioning, possibly even into carrier-specific handsets, making the lock-in into the services of one carrier stronger), thirdly, it seems to create a situation where the US Teleoperators will have facilities available for advanced location-based services much earlier

than in Europe, where the implementation of accurate positioning technologies has not been as quick.

### **3.8. Conclusion**

The discussion and developments in regarding privacy and location information especially in the telecommunications industry has been very active in the past few years.

Outside the authority of FCC, the self-regulatory regime enforced by FTC prevails. In case a company is not under an industry-specific regulations and has not adopted own privacy policy, there is generally very few limitations for the utilisation of personal data.

Within the field of FCC authority FCC has recently adopted detailed rules prescribing the use of CPNI. FCC has not adopted special rules of location information, but has concluded that the request for an express prior authorization under the Telecommunications Act 222 § makes opt-in regime compulsory, and a customer must expressly approve the use of location information.

#### **4. Situation in Japan**

This part of the report is based on the information received during the visit to Japan in March 2002, from The Ministry of Public management, Home Affairs, Post and Telecommunications (SOOMUSHO) and the representatives of Finpro, Tekes and Internet Consortium.

##### **4.1. Data protection regulatory framework overview**

Data protection legislation for telecommunication and position technology does not exist in Japan yet. The general data protection law is now in the Parliament. Data protection in mobile communication and positioning technology is regulated in the general telecommunication legislation and in the data protection guidelines accepted by SOOMUSHO and implemented by the central organization of the telecommunication industry (TCA). The need for legal regulation with regard to data protection is evident, the question being, what kind of legislation is needed. The business and technology is so new that it's difficult to know what kind of legislation is needed.

In addition, there are new regulations related to spamming as well as to liability and responsibility of the Internet Service provider with regard to illegal content of e-mails and www-pages. Furthermore, law concerning electronic signatures and certification services has been passed.

##### Co-operation between Japan and Finland

November last year the Ministry of Public management, Home Affairs, Post and Telecommunications in Japan and The Ministry of Telecommunication and Transportation In Finland have signed an agreement related to the co-operation between Japan and Finland related to developing mobile technology and business (*Finland-Japan joint announcement on mobile Internet, November 15, 2001*).

##### eJapan

Japan has a strategy and a project for the electronic business, eJapan. The goal of eJapan is 'World's most advanced IT nation within 5 years'. In the Policy Program 'Facilitation of eCommerce' one of the priority policies is data protection issues related to the consumer protection.

#### **4.2. Overview of the positioning technology and services utilised**

The position services available in Japan may be categorised into three groups: car navigation, mobile navigation, and vehicle information communication. Different kind of position technology is used, GPS technology and two types of cell-ID technology in the mobile phones, the normal cell phones and Dect-technology that serves for short distance.

The Vehicle Information Communication System that provides traffic information to vehicles is the priority plan of e-Japan. The KDDI, J-phone, NTT Do Co Mo are the main three carriers on the market. The carrier KDDI started to provide services using position technology in December 2000 throughout the country with the brand name 'au'. Only KDDI provides the services, the numbers of users are 434 000. Other than 'au' are NTT DoCoMo's iMode and J-phone's J-Sky/J-navi. J-sky has the system showing the position of the person or exactly the position of the system or the position of technology at the present. The main services are door-to-door guiding, maps, forecasting, city guiding and location based 'notice board'.

The big teleoperators recently started to give the 3<sup>rd</sup> generation services in Japan. The new technology provide more advanced possibilities e.g. to send pictures and e-mails.

#### **4.3. Regulatory bodies for the data protection in the telecommunications field**

The Ministry of Public management, Home Affairs, Post and Telecommunications (SOOMUSHO) is regulatory authority in the telecommunication sector including the data protection and privacy. The Prime Ministry Bureau is responsible of the general Data Protection Code and spamming legislation. The Ministry of Economy, Trade and Industry (METI) is responsible for the legislation concerning the illegal content of the communication. The Tele-

communication Association (TCA) tries to implement the data Protection guidelines of telecommunication. Internet Association/Electronic Internet Consortium represents the Internet Service Providers.

#### **4.4. Data protection regulations for telecommunications and position technology**

##### Introduction

‘The Telecommunication Business Code’ stipulates the confidentiality of telecommunication. The ‘Guidelines on the Protection of Personal data’ includes the principles of information processing related to the users and subscribers as well as location data. There is no special data protection legislation for telecommunication in force yet in Japan. Thus no specified data protection legislation exists related to use of positioning technology and services. From the regulatory authority point of view the situation is open, and location information and the use of location-based services are new issues. The business has been started recently for which reason it is difficult to know the way how the technology will be used. That is why it is too early to draw any detailed conclusions about the issue and it is difficult to say what kinds of rules are relevant and what kind of rules will be implemented in the future. The basic requirement is the confidentiality of the location information. The regulatory work related to telecommunications is waiting for the general data protection law from the parliament. Two recent laws have provisions that include also provisions related to data protection, such laws concerning the responsibility of ISP (Internet Service provider) and spamming.

##### Telecommunication Business Code

*The ‘Telecommunication Business Code’ sets forth the regulatory framework for the provision of the common telecommunication services including telecommunications liberalisation issues. The code stipulates also confidentiality obligation to be implemented within the telecommunication business. To start to provide common telecommunication services a company needs to have the permission of the Minister (Article 9). An agreement with the subscriber is required for the provisions of the service.*

The communications of users and subscribers is confidential. Protection of secrecy is set forth in the Article 4, according to which ‘The communication handled by the carrier shall not be violated’.

### Guidelines of Privacy Protection in Telecommunication

‘The Study Group Privacy Protection in Telecommunication’ has been worked in relation to the Ministry of Posts and Telecommunications (MPT). Now SOOMUSHO has prepared a report by the same name including revision of the ‘Guidelines on the protection of Personal data’. The guidelines are aimed to the telecommunication carriers’ (‘carriers’) use. The number of carriers in the telecommunication business is expected to increase dramatically in the near future, for which reason the importance of the guidelines as well as the worries of the implementation of the privacy protection in services is pointed in the report. Besides telecommunication services are becoming more advanced and diversified. The most important aspect of data protection in such an environment is to appropriate handling of personal data by the carriers to protect the rights of personal privacy. The goal of the Guidelines is to give the principles how to process protection of privacy issues concerning processing personal data in the telecommunication sector on *voluntary basis*. The guidelines are based on the OECD Data Protection guidelines, recommendations of the OECD council concerning ‘Guidelines governing the protection of privacy and transborder flows of Personal Data’ (1980). (Thus the principles are on the line of EU Data Protection directive (95/46/EY) as well as Personal Data Act (523/1999)).

The Article 11 of the guidelines includes principles to process ‘Location information.’ The Association of the telecommunication carriers (TCA) implements issue into the practice. (an Announcement N:o 570, article 11). The clauses of the article 11 includes the prerequisites to disclose location information. The location information is allowed to be disclosed only when the data subject has given his/her consent.

“A telecommunications carrier shall not disclose the location information (the information indicating the location of the party in possession of a mobile terminal) to another except when the **data subject gives consent**, when such disclosure is required by a judge-issued warrant, when such disclosure is a part of tracing the call back (as described the Clause of the 10 article), or when there exists some other legal ground for exception.”

“If a telecommunications carrier provides a service whereby the location data is given to the subscriber or a party designated by the subscriber, or if it discloses the information through a third party, it shall take the necessary measures to prevent the rights of the person possessing the mobile terminal from being improperly violated.”

The guidelines separate a location data related to establish telecommunication service and other location data. The telecommunication data related to the individual calls is protected under the ‘confidentiality of communications’ in the Telecommunication Business Law. The location registration data, which is sent to the station whenever the party is not engaged in a call, these data accumulated at the service control station are to be protected as a matter of privacy. When telecommunication carrier discloses the location information directly or through a third party, carrier should always take into account the prerequisites for such acts. The guidelines say: ‘Must consider carefully the balance with the confidentiality of communications and the protection of privacy’.

In following some basic principles of the guidelines related to processing of location data are introduced. The necessary measures must be taken to ensure that the rights of the users in possession of the mobile terminal shall not be violated. The necessary measures may be included in a contract or an agreement form. According to the received comments the general permission given in a contract is not how to solve the issue. According to the guidelines service provider should always operate within the contents for which *the user of the terminal* has given permission. In case the location-based service is ordered by the subscriber, it should be ensured that the subscriber has the permission of the user of the terminal for the location. If the subscriber (other than the user of the terminal) receives location-based service and the terminal under consideration does not have the property to switch off the transmission of the location information the communication must not be implemented/established, as there is a risk that the rights of the user of the terminal could be violated. Therefore necessary functions of the terminal to turn off the positioning are considered appropriate in such cases. It is further hoped for the mobile terminal to have some indication that the location data can be transmitted and a screen display showing when the location data of the object can be received by others.

Necessary management measures of data includes to set secret codes or to limit access terminals so that a third party cannot monitor the location data of a mobile terminal, if another (second) telecommunications carrier provide the location data service, etc., measures should be taken to set up some guidelines on the management of the data so that a third party is not allowed to use the location data management by the first company.

### Data Protection Code

The Prime Ministry Cabinet in Japan is responsible for '*The General Data Protection Code*' that stipulates the processing of personal data. The general data protection legislation has been given to the parliament two years ago, but the parliament has not yet adopted the legislation. After the Code is accepted by the parliament the sectorial data protection codes will be prepared by the sectorial regulatory bodies e.g. to the financial, medical and telecommunication sector. E.g. SOOMUSHO has thought the issues since three years.)

The Code includes e.g. the statement of the use of person related information. The information may be used only for the defined purpose and only data necessary for the defined purpose may be used, and data may not be disclosed to third parties without permission of the user. The company must inform the user of the purpose of the processing of personal data. The legislation observes the OECD guidelines.

## **4.5. Other related legislation**

### ISP-service provider liability law

The new law concerns the specified telecommunication service providers as well as their responsibility and rights related to the illegal content of the e-mails, www-pages etc. The law on restrictions of the liability for damages specified telecommunications service providers and the right to demand disclosure of identify information of the sender' (Law No: 137) has been given of 30 November 2001 and came into effect in May 2002. The specified telecommunication service providers are e.g. Internet Service Providers (ISP) and the telecommunication e.g. e-mails, home pages.

The law prescribes restrictions on the liability for damages of specified telecommunications service providers and the right to demand disclosure of identity information of the sender in a case where a right is infringed due to the distribution of information by means of specified telecommunications. The specified telecommunication means the communication intended to be received by unspecified person. The legislation includes principles of the rights of the specified telecommunication service provider (e.g. ISP) to prevent the transmission. Besides the law includes the statement that the specified telecommunication service provider has right to disclosure the identity of the sender to the receiver. The Law defines the rights and responsibilities of specified telecommunication service provider and telecommunication service provider.

#### The law related to the misusing telecommunication (Spamming)

The study group has completed a study related to the nuisance e-mail (spamming) January this year 2002 including e.g. the issues of the technical and systematic measurements for controlling and preventing the distribution of nuisance e-mail. On the basis of that work the proposed law on topics including the appropriateness of sending certain designated e-mail has been prepared.

#### **4.6. Summary of the data protection principles**

The telecommunication information is confidential according the Telecommunication Business Code. The practical rules to process telecommunication information are given in the 'Guidelines on the protection of Personal data' but the problem is that the guidelines are not obligatory.

The basic principles are now that only telecommunication carriers are allowed to use location information and provide location-based services using Cell-ID. Because the telecommunication carrier has the right according to the 'Telecommunication Business Code' to use/process the location information related to the transmission of the telecommunication, other companies are providing location-based services via carriers. Only the carrier has the location in-

formation and the carriers provide the services to the users. The service providers are asking the carrier to distribute the services using location information to the users. There is no existing legislation that stipulates the principles for providing services using location information. The Carrier Association is trying to implement 'opt-in' principle. Now the consent is given by the user in the contract what is not relevant for that kind of use.

The 3<sup>rd</sup> Generation will give more possibilities but includes also the risks to violate the privacy. The regulation of the 3<sup>rd</sup> Generation network has not been discussed yet.

#### **4.7. Discussion and views**

Concerning privacy and data protection issues in positioning technology, the 'policy' is open and seems to be the services first – legislation after the problems exists. Probably different kind of possible technologies means also different kinds of regulation. The existing data protection regulation for the telecommunication sector now is very simple and general and not regulated very well.

There seems to be challenges in relation to processing of location data arising from the present practices. There are requests to have legislation for providing harmonized rules for processing location data and providing location-based services. One problem relates to the large databases, e.g. the big telecommunication carriers having large databases consisting information related to the subscribers that they are allowed to use.

The teleoperators may send e-mails to the subscribers or users. E-mail is cheap and very popular, almost every company including banks use e-mails. Encryption is used in the communications and pointed out as a solution for data protection issues, but the common opinion is that the technical security is not the solution for the privacy and data protection. The companies are trying to inform users, but there is no legislation adopted that the companies could follow.

The companies may send advertises to the consumers according the area using cell-ID. The principle is that they ask teleoperator to send the advertising e-mails. Some operators are pro-

viding such advertising services and the other companies are providing content services. The problem is that the customer/consumer does not know when the e-mail is advertising, e.g. a department store sends e-mails about the discounts without the consent and information of the consumer. Spamming may be seen more or less as a social problem.

Also real-time privacy, the usage of the mobile network by the service providers, seems to be a problem. The operators use the information to the other purposes than is allowed. In practice the teleoperator may use the database also of the roaming system. In the press there have been news about cases where teleoperators have been giving information related to the users to other operators without the consent of the user. Privacy issue will be very important in the future. The carriers do not know how they should act, they are waiting for the law. The guidelines are not enough.

## **5. Situation in Italy**

This part of the report is based on information received during the visit from the Data Protection Ombudsman Office (Garante per la protezione dei dati personali) and Mobile Italy Telecom Italy (MIT) in November 2002 Rome, Italy. The Finnish Embassy in Italy co-ordinated the important contacts.

### **5.1. Data protection regulatory framework overview**

The Data Protection Ombudsman Office (Garante per la protezione dei dati personali, hereinafter the“Garante”) is responsible of the general data protection administration and administers also data protection issues related to the provision of publicly available telecommunications services. There are also industry-specific data protection regulations in force. The new data protection legislation in telecommunication sector is currently being prepared to implement the recent EU Directive on the Data Protection in Electronic Communication (2002/58/EC). The aim of the government is to finalise the law proposal before end of this year. In parallel with the preparational work related to the implementation of the directive it is the purpose of the government to collect all data protection regulations to be combined into a one text.

The telecommunications regulatory authorities are responsible for other areas of regulations related to the telecommunication. The Garante has a strong position as a data protection supervisory authority. The representative of the telecommunication company (MIT) stated that when following data protection regulations they are contacting often the data protection authority for additional advise when necessary.

### **5.2. Positioning technology and services overview**

In Italy the utilisation of position technology may be categorised into three main groups: searching location-specific information from yellow pages or corresponding catalogue services (e.g. restaurants), safety systems and equipment of motor vehicles (e.g. used to track a stolen vehicle) that may be required by Insurance Companies, and location-specific advertising.

The position technology used in the provision of the services is usually network-based positioning using cell-ID of terminals, meaning that usually the precision of the information is not high. The yellow page service is based on WAP-technology and is utilising existing web-pages. Only mobile operators are providing services and there are no third-party service providers.

There are approximately 25 million subscribers and 60 million of SIM-cards in Italy. [MITÄ TÄMÄ TARKOITTAA?] . The general data protection legislation includes the basic rules for the process personal information related to process position information. The basic principle is the consent of the user. The implementation of the prerequisite may differ from one service to another depending on the type of the service and purpose to process personal information. [TÄMÄ EHKÄ POISTETAAN?]

### **5.3. Regulatory bodies for the data protection in the telecommunications field**

The Data Protection Ombudsman Office the Office of *Garante* (Garante per la protezione dei dati personali) is the supervisory authority of the Data protection legislation. The Office of Garante is an independent office (Degree by the President of the Republic No. 501 of 31.03.98: Rules of organisation and operation of the Office of the Garante (Supervisory Authority) for the protection of Personal data pursuant to Article 33(3) of the Act no. 675.96. The regulatory bodies of Telecommunication services and licenses are the Ministry of Post and Telecommunication and the Communication Authority. The Ministry of Post and Telecommunication stipulates the Telecommunication service legislation the Communication Authority rules for the Technical licences.

## **5.4. Data protection regulations for telecommunications and position technology**

### Introduction

The Act no. 675 of 31.12.1996 'Protection of individuals and other subjects with regard to the processing of personal data Act' (*General Data Protection Act*) includes sectorial data protection provisions, including provisions related to telecommunications services. In addition, the EU Directive telecommunication data protection directive 97/66/EC is implemented into a special Act no. 171.98 of 13.5.1998.

The general telecommunication legislation 'Legislative Decree no. 197 of 08.05.97, by the Minister for Post and Telecommunications includes regulations with reference to subscription rules and conditions for telephone services. The Decree of 25.11.97 by the Minister for Communications (published on the Official Journal) no. 283 of 04.12.97) includes provisions for granting of individual licences in the telecommunication sector.

### General Data Protection Act

The General Data Protection Act no. 675.96 'Protection of individuals and other subjects with regard to the processing of personal data Act' is aimed for regulating the processing of personal data in the private sector, while the Act no. 676.96 regulates the processing of personal data by the Government. The Acts are among the first implemented data protection regulations based on the General Data Protection Directive 95/46/EC. The General Data Protection legislation 675.96 includes also sectorial rules e.g. for medical and telecommunication sectors. In addition, there are sectorial Data Protection Acts: Act no. 135.99 (Processing of Sensitive Data by Public Bodies), Act no. 282.99 (Medical sector), and the Act no. 171, 13.5.1998 that includes the implementation of the EU Directive 97/66/EC. The Act no. 467 of 28.12.2001 (includes Amendments and Additions to Act 675/1997) stipulates the transfer of data to the other countries and authorisation to use information. The implementation of the new EU Directive of Data Protection on the Electronic Communication (58/2002/EC) is currently being prepared.

The basic principles of General Data Protection Act are similar than those in Finland: the collection and use of person related information s allowed only for specified purposes defined before starting of the processing and use the data is allowed only for these pre-defined purposes. Only necessary information related to the purpose may be collected or processed. In addition, the information may not be disclosed to the third party without the permission of the data subject. The data subject must be informed of the processing of the data.

According the General Data Protection Act 11Article the consent of the Data Subject must fulfil certain minimum criteria : if the consent of the data subject is required for th e processing of personal data, the consent must be documented in writing. In certain cases the Data Subject's consent is not required for the processing of personal data (Article 12), e.g. when there is an agreement between service provider.

It has been concluded that if the user of a mobile terminal is requesting location-specific information (e.g. restaurants) based in his/her present location, he/she has given an implicit consent for processing of his/hers location data.

The 20 Article paragraph a) and a-bis) of the General Data Protection legislation is important in telecommunication:

‘Communication and dissemination of personal data shall be allowed with the data subjects express consent’ (Article 20 a). If they are necessary for the performance of obligations resulting from a contract to which the data subject is a party, or in order to take steps at the data subject's request prior to entering into a contract’ (20 Article a-bis).

The location base service provider has an agreement with the user (Data Subject) related to the use of the services and the consent to process information related to her/him in relation to provision of a location-based service. To transfer/give the location data the provider of a location-based service requires the consent of the data subject. In cases where the user by him/herself asks for the information e.g. about a restaurant the consent is allowed to be implicit. Dissemination of location-specific advertising is allowed if the company has acquired a prior consent for the advertisement (opt-in principle).

In the future there will be both opt-in and opt-out principles in use in Italy for processing of location data. If the company has an agreement with the user of a terminal (customership), and the same company is marketing similar products or services, prior consent for the direct marketing is not required, but the user has a right to prohibit direct marketing (opt-out principle). If there is no customership, the company must ask the consent before sending the direct marketing message (opt-in principle). If such consent is acquired, the presupposition is that it concerns only one message..

### Data Protection Legislation in Telecommunication Sector

The Act no. 171 of 13.5.1998 (includes the principles of EU Directive 97/66/EC) as amended by Act no. 476 of 28.12.01 is separate from the General Data Protection legislation and the implementation of the EU Directive on Data Protection in Electronic Communication (2002/58/EC) is being prepared. The existing legislation includes principles supporting the general data protection act, such as detailed regulations on processing of traffic and billing data and rules and limitations for storing billing data.

According to the existing legislation the use of location data for the services requires the two consent of the person/user.

### Summary of the data protection principles

The General Data Protection Act no. 675.96 'Protection of individuals and other subjects with regard to the processing of personal data Act' is aimed for regulating the processing of personal data in the private sector.

The new EU directive of electronic communication services will be implemented before end of this year 2002. The principles for processing location data and utilising it for location-based services are in the general data protection act. Mobile operators are making agreement with the subscriber/user and store the agreement into the electronic file for the control existence. The agreements of the subscribers are in writing.

It has been concluded that if the user of a mobile terminal is requesting location-specific information (e.g. restaurants) based in his/her present location, he/she has given an implicit consent for processing of his/hers location data. This is because there is an prior agreement between the service provider (the teleoperator and the subscriber) and the user (Data Subject) asks the information by him/her self.

The user may have an agreement with an other company, insurance Company, for getting Insurance to protect the car with the device with SIM and the mobile operator provider the alarming-service (location-based service). The agreement is between the insurance company and user.

The information collected from the location-based services normally is stored to the billing purpose incl. location data. From the supervisory authority's point of view the problem is the long time period of storage of the billing data including location data. The companies do not follow strictly the regulation on storage of data, that is, the provision according to which data may be stored only the period during which a bill may lawfully be challenged or payment may be pursued.

## **5.5. Discussion and views**

The existing legislation in Italy seem to be sufficient from point of view of the regulatory body as well as from the point of view teleopretaor/location-base service providers. The problem is to find solutions that support flexible use of terminal and system.

The police is asking location data and the operators are giving information. The process is acceptable from the point of view of teleoperators but from the supervisory point of view there seems to be problems. It is generally believed that the location data is misused. From the supervisory authority point of view the people do not understand the data protection risks involved in the mobile telecommunications. Teleoperators believe that statements of the data protection legislation are useful. However, even the big operators are requesting more detailed rules.

The problem is the information related to a location of an individual person. The main problem is the connection of information between a location and content. The other problem will be the database that will be maintained by the provider of the location-based service. The basic principle is that database related to the location-based service must be separated from the database of other telecommunication services.

The use of location data by the providers of location-based service requires the consent of the user. The 12 Article includes the rules when the consent of the Data Subject is not needed (the consent is implicit): The consent of the data subject may be implicit in certain cases, as noted earlier.

In the direct marketing both opt-in and opt-out principles are possible.

Currently TIM requires a two-step procedure when of getting the consent for provision of location-based service. Firstly, there is the consent related to an agreement made at the beginning of the customership between the teleoperator and the subscriber for the billing purposes. This information is not transferred to other service providers or companies. The teleoperator is the provider of the location-specific information services (such as yellow pages) and is collecting information for the billing purposes. The information on the nature of the services must be given, after which the user gives his/her consent. When using the service the consent is implicit.

## **6. Situation in Germany**

The part of the report reviews the data protection and privacy regulatory framework in mobile communication and position technology in Germany.

### **6.1. Data Protection in Germany - An Introductory Overview**

In Germany there is the Federal data protection law that has been in effect since 1991, which is a general law on protection of personal data applied to both the public and private sector. As many other legal regulations in Germany the subject of data protection is twofold in a sense that there are public law and private law on the one hand and federal and 'Länder' regulations on the other hand. In addition to the Federal Data Protection Act, which is serving as an omnibus law, there are numerous so-called sector-specific provisions. All these rules are granting the data subject a variety of possibilities aiming at the respect of data protection rights of individuals. There are many special separate laws for many different fields, including telecommunication sector. One opinion is presented that the goal has been to include the specific sectorial legislation into the same text to eliminate in the future situations where two types of regulations provide different levels of protection for same situation.

### **6.2. Regulatory bodies for the data protection in the telecommunications field**

#### Regulatory bodies

In Germany, the Federal legislator (the Federal Ministry of the Interior) is the body primarily responsible for implementation of the General Data Protection Directive in Germany. The Länder laws on the Data Protection are brought into line with Directive. In addition to the general laws on the data protection, a large number of Federal and provisions of the Länder on specific aspects of data protection are included.

The Regulatory Authority for Telecommunications and Posts was set up as provided for by the Telecommunications Act (in force since 1.8.1996). It is a higher federal authority within

the scope of business of the Federal Ministry of Economics and Labour (headquarters in Bonn). The Regulatory Authority superseded the Federal Ministry of Posts and Telecommunications and its subordinate Federal Office. The Regulatory Authority, which took up its work at the beginning of 1998, is responsible for the development of the post and telecommunications markets through liberalisation and deregulation. It has procedures and instruments for the regulatory tasks as well as a set of sanctions. A structurally separate authority with the maximum possible independence is needed to perform these tasks.

#### Supervision and advisory bodies of the data protection

In Germany there are many Data Protection Ombudsmen: The Federal Data Protection Commissioner, the Data Protection Commissioners of the Länder and the supervisory authorities are the bodies responsible for the supervision and monitoring. The supervisory bodies (Data Protection Ombudsman of individual Companies) are the German peculiarity: every enterprise must appoint a data protection Ombudsman (see below for more details).

In 1997 the Federal Data protection Commissioner assumed responsibility for monitoring compliance with data protection rules by companies providing telecommunications services.

### **6.3. Data protection regulations for telecommunications and position technology**

#### General

Earlier the Telecommunications Act included data protection regulations for the field. The data protection law for telecommunication sector was enacted 7.7.1996. The law was revised to conform to the Directive 97/66/EC and the new law was enacted in July 1997 (regarding the basic conditions of the regulations on data communication services, commonly known as the 'multimedia law'. This law comprises three new regulations and revisions to 6 existing regulations, including new legislation on the data protection in tele-services as part of the demands of protecting personal data.

The following are the main legislations related to the data protection in telecommunication data protection field: Telecommunications Act (Telecommunicationsgesetz (TKZ) of 25.6.1996), Telecommunications Carriers Data Protection Ordinance (Telecommunicationsdienstunternehmen-Datenschutzverordnung (TDSV) of 12.8.1996), the Information and Communication Services Law (Informations- und Kommunikationsdienst-Gesetz) was adopted in June 1997. The Telecommunications Customer Protection Decree (Telecommunications-Kundenschutzverordnung of 11.12.1997) entered into force in January 1998. The specified regulation on principles for disclosing location data to third parties does not exist yet.

### Telecommunication Act

The purpose of *Telecommunication Act (TKZ)* is to promote competition, to guarantee appropriate and adequate services throughout the country and to provide for frequency regulation. The law includes also the provisions of data protection.

### General Data Protection Act

The Federal Data Protection Act (Bundesdatenschutz (BDSG)) adopted in the year 2000 December, entered into force 23.5.2001. The Federal Data Protection Act is separate to the private enterprises and public bodies. The Act includes the implementation of the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Act). In Germany there are 16 Länders it seems to be that part of them have yet adopted new data protection legislations pursuant to the Directive. ([http://europa.eu.int/comm/internal\\_market/en/dataprotection/law](http://europa.eu.int/comm/internal_market/en/dataprotection/law)). Thus the Federal Data Protection Act as well as the laws of Länders will include the same principles than directive 95/46/EC as well as the Personal Data Act in Finland but there are differences related to the structures and also content. Giving an overall view of the requirements of data protection legislation in Germany is extremely difficult due to the number of applicable regulations in different levels and different fields.

There is in the first place the right of an individual to review registered data. Private organizations (also public sector) must on request provide the data subject with details of the data

they hold on him (sect. 19 and 34 of the Federal Data Protection Act (BDSG). The Federal Data Protection Commissioner must keep a register of electronic systems (registers) containing personal information, which the public may consult (Sect. 26 par. 5). When automated processing procedures are taken into use, by the telecommunications companies, they have to register such procedures with Federal Commissioner for data protection (in accordance with section 4c). The exceptions are situations presented in Section 4d, e.g. when information is stored only for purpose of transfer or purpose of anonymised transfer. The right of notification (sect. 33) ensures that data subjects are always aware of who is processing which data of a person and to which purpose. Every system or register containing personal data must be defined by the controller of the file. These regulations are in line with the General Data Protection Directive and the Finnish Personal Data Act.

The basic prerequisites to collect information from the certain person according the Federal Data Protection Act (BDSG) is the given information to the person and the consent given by the person. The information must be given before obtaining the consent. The consent must be distinguishable in its appearance, e.g. if the consent is to be given together with other written document/declarations. Also to transfer personal-related information to the outsider the consent is required (unless otherwise provided by the law). The information must be given also if information is collected without data subject's knowledge.

The Federal Data Protection Act includes prerequisites of process information to the competition issues e.g. marketing, advertising etc., that means the prerequisites to process information to other purposes than customership, employment, membership etc. The statements are concerning e.g. rights of the data subject (notification to the data subject, request by the data subject to get access to the stored information from him/her) and supervisory authority (that monitor the implementation).

#### **6.4. Supervisory authorities – data protection ombudsman of enterprises**

Every private (also public) bodies are obliged to appoint a data protection ombudsman within one month of commencing their activities to collect and process information. There are certain exceptions e.g. concerning amount of the employees. When private bodies carry out

automated processing operations which are subject to prior checking or collect process or use personal data in the course of business for the purposes of transfer or anonymised transfer, they are to appoint a data protection official irrespective of the number of employees. The Act includes the requirements of the person who may be appointed data protection official. A person from the outside the company may also be entrusted with this duty that is the case normally in small companies. The big companies such as telecommunication companies may have several ombudsmen. The requirement is also that the data protection official must be directly subordinate to the head of the company. The company must support the data protection official in his/her duty and make all necessary arrangements. Data subjects may approach the data protection official at any time. The official may educate the personnel of the controller, check that the systems are functioning properly, contact to data protection authorities e.g.

### **6.5. Data Protection Legislation in Telecommunication Sector**

Telecommunications Data Protection Ordinance (TDSV) of 18.12.2000 on the base on the Telecommunication Act (89 §) 25.6.1996) and includes the implementation of directive 97/66/EC. The Ordinance regulating Data Protection for Telecommunication Carriers, 12.6.1996 expires at the same time).

The TDSV (89 §) includes the basic principles of data protection in telecommunication. The processing of personal information to other purposes than establish a communication is based on the consent of the user/subscriber. Customer data already collected by the company may be processed for marketing if the user has not prohibited such use (opt-out principle). If the user is asked to give his consent the information must be given clearly about what the consent means e.g. content and scope. TDSV definition of the traffic data a service provider are allowed to collect includes the position when mobile station are used. The basic principle is the data must be destroyed after communication completed but allowed to use e.g. the necessary information to billing.

## APPENDICES

### APPENDIX 1

#### REFERENCES FOR THE REPORT CONCERNING USA

The report concerning USA is based on review of legislation, current articles and privacy literature, as well as on information provided by FCC, the interest groups. Important has also been the expert opinions received. The following experts were met in relation to the making of this report:

Mr Cary Mitchell, Law Firm Blooston, Mordkofsky, Dickens, Duffy & Prendergast.

Mr Mitchell is a telecommunications lawyer who has a great interest in positioning technology. He was indispensable help in organising the meetings during the visit. He was also the first person to provide us with the first general overview of the current situation in USA.

Mr. Peter Swire, George Washington University Law School.

From March, 1999 until January 2001 Peter Swire served as the President Clinton Administration's Chief Counsellor for Privacy, in the USA States Office of Management and Budget. In early January Mr. Swire returned to his position as professor of Law at the Ohio State University College of Law. He is now a Visiting Professor of Law at the George Washington University Law School.

The topic of our discussion was especially the general Privacy Framework in USA and the differences between EU and USA – specially Safe Harbour arrangement.

Mr. David L. Sobel, General Council in EPIC ([www.epic.org](http://www.epic.org)).

Mr. Charles H. Kennedy, attorney-at-law, Morrison & Foerester LLP.

Mr Kennedy is one of the leading experts in the telecommunications regulation. He has participated in several publications in the field. With his colleague he provided a written testimony to the House Subcommittee on Trade and Consumer Protection in May of 2001 on the Topic of Impediments to Digital Trade, where he also addressed privacy issues related to the

digital trade. In the testimony he urged the U.S. Government to adopt a 'Safe Harbour Privacy Accord' that creates a single privacy regime for U.S companies to follow to assure compliance with the EU Directive on Data Protection when transferring personal information from the EU to US.

Ms. Marcy Greene, Attorney Advisor for the Federal Communications Commission (FCC), and Ms. Kris Monteith, Chief Policy Division for the Wireless Telecommunications Bureau of FCC.

FCC is the executive body in the USA for regulation related to telecommunications. Ms. Green is the attorney responsible for the FCC's efforts to implement the customer Proprietary Network Information (or. 'CPNI') provision (Section 222) of the Telecommunication Act.

So called "ex party notification" had to be filed for the meeting. The notification is accessible from FCC pages ([www.fcc.gov](http://www.fcc.gov), e-filing system).

Mr. Michael F. Altschul, Senior Vice President and General Counsel, Cellular Telecommunications & Internet Association (CTIA).

CTIA is the most influential interest group in the field of telecommunications representing the wireless carriers operating in the USA. As the general counsel of CTIA Mr Altschul is probably the best expert to express the views of CTIA in the matter relating to the privacy regulations.

Mr. John W. Jimison, General Council at Wireless Location Industry Association (WLIA).

WLIA is an organisation representing companies involved in the development and provision of location services. WLIA has been developing its own privacy principles. WLIA will require adherence to the adopted privacy principles from its members. The goal is to be able to develop a widely accepted self-regulative system for the utilisation of location data.

## APPENDIX 2

### REFERENCES FOR THE REPORT RELATED TO JAPAN

#### Visitit Tokio Japan 5.-8.3.2002

##### **Finnish Embassy in Japan.**

Mr. Markkanen ,The Concellor (co-ordinator)

##### **The Ministry of Public management, Home Affairs, Post and Telecommunications (SOOMUSHO).**

*Shijeki SUZUKI*, Director, International Economic Affairs Division, Telecommunication Burea

*Mr. Hirosato HAYASHI*, Deputy Director, Internationa Economic Affairs Division

*Mr. Hiroyuki OHUSAGA*, Attorney, Deputy Dierctor of Telecommunications Consumers Affairs Office Telecommunication Business Department , Telecommunication Bureau

*Mr. Shunshi Ohta*, Electronic Network Consortium, Internet Association Japan,

##### **Tekes**

*Eichi Washisu*, Technology consultant, Tekes

##### **Finpro**

Coichi Tanaka, Commercial officer of Finpro

##### **Electronic Network Consortium**

*Mr. Shunshi Ohta*

##### **White paper 2002**

‘Information and Communications in Japan, Stirring of the IT-prevalent Society, ,, Ministry of Public Management, Home Affairs, Post and Telecommunications, Japan (Web-site of SOOMUSHO)

## APPENDIX 3

### EXTRACT FROM FCC DOCUMENTATION CONCERNING E911 TIMETABLE

#### BACKGROUND

*This appendix contains extracts from FCC decisions concerning e911 timetable. According to FCC Teleoperartors have been divided generally to three categories: (i) certain nation-wide Teleoperators who have proposed their own a roll-out timetable for the Phase II of e911, which FCC has accepted (“Tier I” carrier, AT&T as an example below) (ii) other Teleoperators with more than 500.000 subscribers (“Tier II”), and (iii) Teleoperators with less than 500.000 subscribers (“Tier III”).*

*NOTE: the numbering of the extracts does not correspond to the original.*

#### AT&T Wireless (example of Tier I Carrier)

AT&T Wireless’ request to deploy E-OTD technology for its GSM network is granted, subject to compliance with the specific conditions set forth below. Because E-OTD requires handset modifications to be effective, AT&T will be subject to all of the requirements applicable to handset-based technologies except as specifically waived or modified in this order.

- Effective October 1, 2001, AT&T’s E-OTD-capable handsets must provide ALI with an accuracy of 100 meters/67 percent of calls and 300 meters/95 percent of calls.
- Effective October 1, 2003, AT&T’s E-OTD-capable handsets activated on or thereafter must comply with an accuracy of 50 meters/67 percent of calls and 150 meters/95 percent of calls.

To the extent AT&T cannot comply with these accuracy requirements, AT&T must use another ALI methodology that comports with the accuracy requirements of the Commission’s rules.

#### Tier II Carriers

1. *Phase-in for network-based location technologies.* Licensees who employ a network-based location technology shall provide Phase II 911 enhanced service to at least 50 percent of the PSAP’s coverage area or population beginning **March 1, 2003** (approximately seven months from the date of this Order), or within 6 months of a PSAP request, whichever is later; and to 100 percent of the PSAP’s coverage area or population by **March 1, 2004** or within 18 months of such a request, whichever is later.

2. *Phase-in for handset-based location technologies.* Licensees who employ a handset-based location technology may phase in deployment of Phase II enhanced 911 service,

subject to the following requirements:

- (1) Without respect to any PSAP request for deployment of Phase II 911 enhanced service, the licensee shall:
  - (i) Begin selling and activating location-capable handsets no later than **March 1, 2003**;
  - (ii) Ensure that at least 25 percent of all new handsets activated are location-capable no later than **May 31, 2003**;
  - (iii) Ensure that at least 50 percent of all new handsets are location-capable no later than **November 30, 2003**; and
  - (iv) Ensure that 100 percent of all new digital handsets activated are location-capable no later than **May 31, 2004**.
  - (v) Ensure that penetration of location-capable handsets among its subscribers reaches 95 percent no later than December 31, 2005.
  
- (2) Once a PSAP request is received, the licensee shall, in the area served by the PSAP, within six months or by **March 1, 2003**, whichever is later:
  - (i) Install any hardware and/or software in the CMRS network and/or other fixed infrastructure, as needed, to enable the provision of Phase II enhanced 911 service; and
  - (ii) Begin delivering Phase II enhanced 911 service to the PSAP.

### **Tier III Carriers**

3. *Phase-in for network-based location technologies.* Licensees who employ a network-based location technology shall provide Phase II 911 enhanced service to at least 50 percent of the PSAP's coverage area or population beginning **September 1, 2003** (approximately thirteen months from the date of this Order), or within 6 months of a PSAP request, whichever is later; and to 100 percent of the PSAP's coverage area or population by **September 1, 2004** or within 18 months of such a request, whichever is later.

4. *Phase-in for handset-based location technologies.* Licensees who employ a handset-based location technology may phase in deployment of Phase II enhanced 911 service, subject to the following requirements:

- (1) Without respect to any PSAP request for deployment of Phase II 911 enhanced service, the licensee shall:
  - (i) Begin selling and activating location-capable handsets no later than **September 1, 2003**;

- (ii) Ensure that at least 25 percent of all new handsets activated are location-capable no later than **November 30, 2003**;
  - (iii) Ensure that at least 50 percent of all new handsets are location-capable no later than **May 31, 2004**; and
  - (iv) Ensure that 100 percent of all new digital handsets activated are location-capable no later than **November 30, 2004**.
  - (v) Ensure that penetration of location-capable handsets among its subscribers reaches 95 percent no later than December 31, 2005.
- (2) Once a PSAP request is received, the licensee shall, in the area served by the PSAP, within six months or by **September 1, 2003**, whichever is later:
- (i) Install any hardware and/or software in the CMRS network and/or other fixed infrastructure, as needed, to enable the provision of Phase II enhanced 911 service; and
  - (ii) Begin delivering Phase II enhanced 911 service to the PSAP.

## APPENDIX 4

### FCC RULES FOR THE USE OF THE CUSTOMER PROPRIETARY NETWORK INFORMATION

#### § 64.2001 Basis and Purpose.

(a) *Basis.* The rules in this subpart are issued pursuant to the Communications Act of 1934, as amended.

(b) *Purpose.* The purpose of the rules in this subpart is to implement section 222 of the Communications Act of 1934, as amended, 47 U.S.C. § 222.

#### § 64.2003 Definitions.

Terms in this subpart have the following meanings:

(a) *Affiliate.* The term "affiliate" has the same meaning given such term in section 3(1) of the Communications Act of 1934, as amended, 47 U.S.C. § 153(1).

(b) *Communications-related services.* The term "communications-related services" means telecommunications services, information services typically provided by telecommunications carriers, and services related to the provision or maintenance of customer premises equipment.

(c) *Customer.* A customer of a telecommunications carrier is a person or entity to which the telecommunications carrier is currently providing service.

(d) *Customer proprietary network information (CPNI).* The term "customer proprietary network information (CPNI)" has the same meaning given to such term in section 222(h)(1) of the Communications Act of 1934, as amended, 47 U.S.C. § 222(h)(1).

(e) *Customer premises equipment (CPE).* The term "customer premises equipment (CPE)" has the same meaning given to such term in section 3(14) of the Communications Act of 1934, as amended, 47 U.S.C. § 153(14).

(f) *Information services typically provided by telecommunications carriers.* The phrase "information services typically provided by telecommunications carriers" means only those information services (as defined in section 3(20) of the Communications Act of 1934, as amended, 47 U.S.C. § 153(2)) that are typically provided by telecommunications carriers, such as Internet access or voice mail services. Such phrase "information services typically provided by telecommunications carriers," as used in this subpart, shall not include retail consumer services provided using Internet websites (such as travel reservation services or mortgage lending services), whether or not such services may otherwise be considered to be information services.

(g) *Local exchange carrier (LEC).* The term "local exchange carrier (LEC)" has the same meaning given to such term in section 3(26) of the Communications Act of 1934, as amended, 47 U.S.C. § 153(26).

(h) *Opt-in approval.* The term "opt-in approval" refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. This approval method requires that the carrier obtain from the customer affirmative, express consent allowing the requested CPNI usage, disclosure, or access after the customer is provided appropriate notification of the carrier's request consistent with the requirements set forth in this subpart.

(i) *Opt-out approval.* The term "opt-out approval" refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's CPNI if the customer has failed to object thereto within the waiting period described in section 64.2009(d)(1) of this subpart, after the customer is provided appropriate notification of the carrier's request for consent consistent with the rules in this subpart.

(j) *Subscriber list information (SLI).* The term "subscriber list information (SLI)" has the same meaning given to such term in section 222(h)(3) of the Communications Act of 1934, as amended, 47 U.S.C. § 222(h)(3).

(k) *Telecommunications carrier or carrier.* The terms "telecommunications carrier" or "carrier" shall have the same meaning as set forth in section 3(44) of the Communications Act of 1934, as amended, 47 U.S.C. § 153(44).

(l) *Telecommunications service.* The term "telecommunications service" has the same meaning given to such term in section 3(46) of the Communications Act of 1934, as amended, 47 U.S.C. § 153(46).

#### § 64.2005 Use of Customer Proprietary Network Information Without Customer Approval.

(a) Any telecommunications carrier may use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service (*i.e.*, local, interexchange, and CMRS) to which the customer already subscribes from the same carrier, without customer approval.

(1) If a telecommunications carrier provides different categories of service, and a customer subscribes to more than one category of service offered by the carrier, the carrier is

permitted to share CPNI among the carrier's affiliated entities that provide a service offering to the customer.

(2) If a telecommunications carrier provides different categories of service, but a customer does not subscribe to more than one offering by the carrier, the carrier is not permitted to share CPNI with its affiliates, except as provided in section 64.2007(b).

(b) A telecommunications carrier may not use, disclose, or permit access to CPNI to market to a customer service offerings that are within a category of service to which the subscriber does not already subscribe from that carrier, unless that carrier has customer approval to do so, except as described in paragraph (c) of this section.

(1) A wireless provider may use, disclose, or permit access to CPNI derived from its provision of CMRS, without customer approval, for the provision of CPE and information service(s). A wireline carrier may use, disclose or permit access to CPNI derived from its provision of local exchange service or interexchange service, without customer approval, for the provision of CPE and call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion.

(2) A telecommunications carrier may not use, disclose or permit access to CPNI to identify or track customers that call competing service providers. For example, a local exchange carrier may not use local service CPNI to track all customers that call local service competitors.

(c) A telecommunications carrier may use, disclose, or permit access to CPNI, without customer approval, as described in this subparagraph (c).

(1) A telecommunications carrier may use, disclose, or permit access to CPNI, without customer approval, in its provision of inside wiring installation, maintenance, and repair services.

(2) CMRS providers may use, disclose, or permit access to CPNI for the purpose of conducting research on the health effects of CMRS.

(3) LECs and CMRS providers may use CPNI, without customer approval, to market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain centrex features.

(d) A telecommunications carrier may use, disclose or permit access to CPNI to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

**§ 64.2007 Approval Required for Use of Customer Proprietary Network Information.**

(a) A telecommunications carrier may obtain approval through written, oral or electronic methods.

(1) A telecommunications carrier relying on oral approval shall bear the burden of demonstrating that such approval has been given in compliance with the Commission's rules in this part.

(2) Approval or disapproval to use, disclose, or permit access to a customer's CPNI obtained by a telecommunications carrier must remain in effect until the customer revokes or limits such approval or disapproval.

(3) A telecommunications carrier must maintain records of approval, whether oral, written or electronic, for at least one year.

*(b) Use of Opt-Out and Opt-In Approval Processes.*

(1) A telecommunications carrier may, subject to opt-out approval or opt-in approval, use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer. A telecommunications carrier may, subject to opt-out approval or opt-in approval, disclose its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, to (i) its agents, (ii) its affiliates that provide communications-related services, and (iii) its joint venture partners and independent contractors. A telecommunications carrier may also permit such persons or entities to obtain access to such CPNI for such purposes. Any such disclosure to or access provided to joint venture partners and independent contractors shall be subject to the safeguards set forth below in paragraph (2) of this subsection (b).

(2) *Joint Venture/Contractor Safeguards.* A telecommunications carrier that discloses or provides access to CPNI to its joint venture partners or independent contractors shall enter into confidentiality agreements with independent contractors or joint venture partners that comply with the following requirements. The confidentiality agreement shall: (A) require that the independent contractor or joint venture partner use the CPNI only for the purpose of marketing or providing the communications-related services for which that CPNI has been provided; (B) disallow the independent contractor or joint venture partner from using, allowing access to, or disclosing the CPNI to any other party, unless required to make such disclosure under force of law; (C) require that the independent contractor or joint venture partner have appropriate protections in place to ensure the ongoing confidentiality of consumers' CPNI.

(3) Except for use and disclosure of CPNI that is permitted without customer approval under section 64.2005, or that is described in paragraph (1) of this section, or as otherwise provided in section 222 of the Communications Act of 1934, as amended, a telecommunications carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval.

**§ 64.2008 Notice Required for Use of Customer Proprietary Network Information**

(a) *Notification, Generally.* (1) Prior to any solicitation for customer approval, a telecommunications carrier must provide notification to the customer of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI.

(2) A telecommunications carrier must maintain records of notification, whether oral, written or electronic, for at least one year.

(b) Individual notice to customers must be provided when soliciting approval to use, disclose, or permit access to customers' CPNI.

(c) *Content of Notice.* Customer notification must provide sufficient information to enable the customer to make an informed decision as to whether to permit a carrier to use, disclose, or permit access to, the customer's CPNI.

(1) The notification must state that the customer has a right, and the carrier has a duty, under federal law, to protect the confidentiality of CPNI.

(2) The notification must specify the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time.

(3) The notification must advise the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and must clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes. However, carriers may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI.

(4) The notification must be comprehensible and must not be misleading.

(5) If written notification is provided, the notice must be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to a customer.

(6) If any portion of a notification is translated into another language, then all portions of the notification must be translated into that language.

(7) A carrier may state in the notification that the customer's approval to use CPNI may enhance the carrier's ability to offer products and services tailored to the customer's needs. A carrier also may state in the notification that it may be compelled to disclose CPNI to any person upon affirmative written request by the customer.

(8) A carrier may not include in the notification any statement attempting to encourage a customer to freeze third-party access to CPNI.

(9) The notification must state that any approval, or denial of approval for the use of CPNI outside of the service to which the customer already subscribes from that carrier is valid until the customer affirmatively revokes or limits such approval or denial.

(10) A telecommunications carrier's solicitation for approval must be proximate to the notification of a customer's CPNI rights.

(d) *Notice Requirements Specific to Opt-Out.* A telecommunications carrier must provide notification to obtain opt-out approval through electronic or written methods, but not by oral communication (except as provided in paragraph (f) of this section). The contents of any such notification must comply with the requirements of subsection (c) of this section.

(1) Carriers must wait a 30-day minimum period of time after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI. A carrier may, in its discretion, provide for a longer period. Carriers must notify customers as to the applicable waiting period for a response before approval is assumed.

(A) In the case of an electronic form of notification, the waiting period shall begin to run from the date on which the notification was sent.

(B) In the case of notification by mail, the waiting period shall begin to run on the third day following the date that the notification was mailed.

(2) Carriers using the opt-out mechanism must provide notices to their customers every two years.

(3) Telecommunications carriers that use e-mail to provide opt-out notices must comply with the following requirements in addition to the requirements generally applicable to notification:

(A) carriers must obtain express, verifiable, prior approval from consumers to send notices via e-mail regarding their service in general, or CPNI in particular;

(B) carriers must allow customers to reply directly to e-mails containing CPNI notices in order to opt-out;

(C) opt-out e-mail notices that are returned to the carrier as undeliverable must be sent to the customer in another form before carriers may consider the customer to have received notice; and

(D) carriers that use e-mail to send CPNI notices must ensure that the subject line of the message clearly and accurately identifies the subject matter of the e-mail.

(E) Telecommunications carriers must make available to every customer a method to opt-out that is of no additional cost to the customer and that is available 24 hours a day, seven days a week. Carriers may satisfy this requirement through a combination of methods, so long as

all customers have the ability to opt-out at no cost and are able to effectuate that choice whenever they choose.

(c) *Notice Requirements Specific to Opt-In.* (1) A telecommunications carrier may provide notification to obtain opt-in approval through oral, written, or electronic methods. The contents of any such notification must comply with the requirements of subsection (c) of this section.

(f) *Notice Requirements Specific to One-Time Use of CPNI.* Carriers may use oral notice to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call, regardless of whether carriers use opt-out or opt-in approval based on the nature of the contact.

(1) The contents of any such notification must comply with the requirements of subsection (c) of this section, except that telecommunications carriers may omit any of the following notice provisions if not relevant to the limited use for which the carrier seeks CPNI:

(A) carriers need not advise customers that if they have opted-out previously, no action is needed to maintain the opt-out election.

(B) carriers need not advise customers that they may share CPNI with their affiliates or third parties and need not name those entities, if the limited CPNI usage will not result in use by, or disclosure to, an affiliate or third party.

(C) carriers need not disclose the means by which a customer can deny or withdraw future access to CPNI, so long as carriers explain to customers that the scope of the approval the carrier seeks is limited to one-time use.

(D) carriers may omit disclosure of the precise steps a customer must take in order to grant or deny access to CPNI, as long as the carrier clearly communicates that the customer can deny access to his CPNI for the call.

#### **§ 64.2009 Safeguards Required for Use of Customer Proprietary Network Information**

(a) Telecommunications carriers must implement a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI.

(b) Telecommunications carriers must train their personnel as to when they are, and are not, authorized to use CPNI, and carriers must have an express disciplinary process in place.

(c) All carriers shall maintain a record, electronically or in some other manner, of their own and their affiliates' sales and marketing campaigns that use their customers' CPNI. All carriers shall maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record must include a description of each campaign, the specific CPNI that was used in the campaign, and what

products and services were offered as a part of the campaign. Carriers shall retain the record for a minimum of one year.

(d) Telecommunications carriers must establish a supervisory review process regarding carrier compliance with the rules in this subpart for outbound marketing situations and maintain records of carrier compliance for a minimum period of one year. Specifically, sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval.

(e) A telecommunications carrier must have a corporate officer, as an agent of the carrier, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the rules in this subpart. The carrier must provide a statement accompanying the certificate explaining how its operating procedures ensure that it is, or is not, in compliance with the rules in this subpart.

(f) Carriers must provide written notice within five business days to the Commission of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

(1) The notice shall be in the form of a letter, and shall include the carrier's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to customers, and contact information.

(2) Such notice must be submitted even if the carrier offers other methods by which consumers may opt-out.

**APPENDIX 5****REFERENCES FOR THE REPORT CONCERNING ITALY****Vistit Italy Rome 8.11.2002**

Finnish Embassy in Italy (Co-ordinator)

**Garante per la Privacy dei Dati Personali (Data Protection Ombudsman Office)**

Piazza Montecitorio 121, 00186 Roma , Mrs. Stefanina Conciensa, Mr.

**Telecom Italy Mobile, TIM-Gruppo**

Mr. Aldo Ancora, Affari Legali e Societari Dritto Pubblico