

Positioning technology: Current Regulatory Framework

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



Report of the NAVI Regulatory Framework -project

**Positioning technology:
Current Regulatory Framework**

Samuli Simojoki

Report of the NAVI Regulatory Framework -project

Publisher:

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

Yhteenveto

Executive Summary

1. Background of the Report	11
2. Relevant fields of Regulation.....	13
2.1. <i>What is positioning technology and how is it utilised?</i>	13
2.2. <i>Positioning Technology: Legal Perspective</i>	14
2.3. <i>Classification of Location-based Services</i>	15
2.4. <i>Concepts</i>	18
3. Different methods for generating Location Data in the Light of Data Protection Regulations.....	18
3.1. <i>Central Data Protection Legislation</i>	18
3.2. <i>Methods for Generating Location Data</i>	19
3.3. <i>Location Data within the framework of the Tele Privacy Act</i>	21
3.4. <i>Applicability of the Tele Privacy Act and the Personal Data Act</i>	22
3.5. <i>Choice of Law</i>	27
3.6. <i>Conclusion: the Applicable Law in Generating Location Data</i>	29
4. Renewal of the European Regulations on Electronic Communications.....	29
4.1. <i>Background</i>	29
4.2. <i>Regulations Concerning Traffic Data</i>	31
4.3. <i>Location Data Processed within the Teleinfrastructure</i>	34
4.4. <i>Location Data – Traffic Data</i>	36
4.5. <i>Location Data Processed by Providers of Location-based Services</i>	37
4.6. <i>Distinction of a User and Subscriber</i>	39
4.7. <i>Obligations of Teleoperator or Value Added Service Provider?</i>	39
4.8. <i>Conclusion</i>	39
5. Utilisation and Processing of Location Data.....	40
5.1. <i>General Remarks</i>	40
5.2. <i>General Principles of the Personal Data Act</i>	45
5.3. <i>Prerequisites for Processing of Personal Data</i>	45
5.4. <i>Consent, Assignment and Relevant Connection</i>	47

5.5.	<i>Consent for Processing of Location Data by a Service Provider</i>	51
5.6.	<i>Special Cases: Continuous Positioning and Monitoring</i>	54
5.7.	<i>Transfer of Location Data Between Teleoperators</i>	57
5.8.	<i>Transfer of Location Data between a Teleoperator and a Service Provider</i>	60
5.9.	<i>Internal Processing of Location Data by the Teleoperator or Service Provider</i>	65
5.10.	<i>Positioning Technology and the Finnish Criminal Code</i>	66
6.	Intellectual Property Rights Issues Related to Positioning Technology	67
6.1.	<i>Content Production and IPR – Overview</i>	68
6.2.	<i>Spatial Data and IPR</i>	70
6.3.	<i>Location Data and IPR</i>	72
6.4.	<i>Utilisation of Public Information Resources</i>	73
7.	Liability Questions Pertaining to the Provision of Positioning Services and Location-based Services	74
7.1.	<i>Different grounds for Damage liability</i>	74
7.2.	<i>Contractual Liability</i>	75
7.3.	<i>Public Services</i>	78
8.	Contractual Issues Related to Provision of Positioning Services and Location-based Services	79
8.1.	<i>Contracting parties</i>	80
8.2.	<i>Contract Formation</i>	81
8.3.	<i>Cancelling the offer</i>	83
8.4.	<i>Electronic Signature</i>	83
8.5.	<i>Choice of Law</i>	84
8.6.	<i>Other aspects of consumer protection</i>	86
9.	Utilisation Of Positioning Technology In Certain Fields	88
9.1.	<i>Provision of Information Society Services</i>	88
9.2.	<i>New Act Concerning Freedom of Speech</i>	92
9.3.	<i>Protection Of Privacy In Employment Relations</i>	93
9.4.	<i>Positioning Of Persons under Guardianship and Elderly People</i>	94
9.5.	<i>Positioning Technology in Direct Marketing</i>	95

Voimassaolevat säädöspuitteet –raportti

Suomenkielinen yhteenveto¹

Sovellettava laki ja tietosuoja

Yleinen henkilötietojen käsittelyä koskeva laki Suomessa on henkilötietolaki. Siltä osin kun sijaintitieto koskee tunnistettavissa olevaa henkilöä, on kyseessä henkilötieto, ja tiedon käsittelyssä on noudatettava henkilötietolakia. Henkilötietolaki on yleislaki, jota on sovellettava jos muuta ei ole säädetty. Monilla aloilla on oma erityinen tietosuojanormisto.

Toinen tärkeä sovellettava normisto Suomessa on teletoiminnan tietosuojalaki (laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta, 565/1999), joka koskee muun muassa verkkoviestinnän tietosuojakysymyksiä.

EU:ssa on heinäkuussa 2002 hyväksytty uusi viestintäverkkojen tietosuojadirektiivi osana laajaa viestintäverkkojen sääntelyn kokonaisuudistusta. Uusi direktiivi muuttaa tietosuojanormistoa merkittävästi. Direktiivi sisältää nimenomaisia sijaintitiedon käsittelyä koskevia määräyksiä. Direktiivin implementointi tulee selkeyttämään sijaintitiedon käsittelyä koskevaa säädösympäristöä. Siirtymäaikana ennen direktiivin implementointia olisi toivottavaa, että nykyistä normistoa voitaisiin siinä määrin kuin mahdollista tulkita direktiivin määräysten valossa.

Sijaintitiedon hyödyntäminen

Yleisesti ottaen on sijaintitiedon generoimismenetelmät voidaan jakaa kahteen luokkaan:

- verkkopaikannus
- laitepaikannus

¹ Suomenkielinen yhteenveto ja Englanninkielinen executive summary eivät ole identtisiä

Verkkopaikannuksessa teleoperaattorin asema on keskeinen, sillä teleoperaattori generoi sijaintitiedon ja kontrolloi siten sen jakelua. Laittepaikannuksessa sijaintitieto syntyy käyttäjän päätelaitteelle, ja käyttäjä kontrolloi sijaintitiedon jakamista itse.

Verkkopaikannuksen keskeiset kysymykset kohdistuvat juuri teleoperaattorin rooliin: esim. milloin teleoperaattori saa hyödyntää sijaintitietoa tai luovuttaa sen kolmansille?

Käyttäjän suostumus

Tässä raportissa esitetään, että yleensä käyttäjän riittävän informoitu ja tietoinen suostumus on riittävä edellytys sijaintitiedon hyödyntämiseen ja luovuttamiseen, ja että joissain tapauksissa paikkaperusteisen palvelun tilaaminen voi sellaisenaan perustaa tällaisen suostumuksen ilman erillistä vahvistusta. Tämä on tilanne erityisesti silloin, jos sijaintitiedon hyödyntäminen palvelun tarjoamisessa on itsestään selvää palvelun luonne huomioon ottaen. On toivottavaa, että direktiivin implementoinnissa selkeytetään suostumukselle eri tilanteissa asetettavia kriteereitä.

Tarvittavan informaation tarjoaminen käyttäjälle tulisi huomioida jo aikaisessa vaiheessa palveluita suunniteltaessa.

Jatkuvaa paikannusta edellyttäviin ja seurannan mahdollistaviin palveluihin liittyy erityisiä tietosuojuongelmia. Nämä riskit voidaan pitkälti välttää suunnittelemalla palvelut järkevästi. Jatkuvan paikannuksen ja seurannan erityiskysymykset voitaisiin huomioida esimerkiksi käyttäjän päätelaitteelle lähetettävillä ajoittaisilla muistutuksilla.

Verkkopaikannuksessa palveluntarjoajan (=teleoperaattorista erillinen taho, joka tarjoaa paikkaperusteista palvelua) on saatava Teleoperaattorilta sijaintitieto. Siksi palveluntarjoajan on noudatettava Teleoperaattorin asettamia teknisiä ja menettelyllisiä määräyksiä. Teleoperaattorit asettavat määräykset niin, että voivat itse täyttää Teleoperaattorin ja käyttäjän välillä olevan asiakassuhteen tietosuojaan liittyvät velvoitteet. Käyttäjän suostumuksen varmistamiseen on käytettävissä lukuisia eri vaihtoehtoja.

Sijaintitiedon luovuttamisessa palveluntarjoajalle pitäisi riittää, että teleoperaattori on tavalla tai toisella varmistanut, että käyttäjä on antanut suostumuksensa sijaintitiedon luovuttamiseen palveluntarjoajalle. Toisin sanoen teleoperaattorille ei pidä asettaa vastuuta sijaintitiedon käytöstä palveluntarjoajan toimesta, kuten esim. käyttötarkoituusspesifin suostumuksen edellytystä sijaintitiedon luovuttamiselle. Sijaintitiedon käsittelyn tarkoitus ja samalla myös sijaintitiedon käsittelyn rajat määräytyvät käyttäjän ja palveluntarjoajan välisen suhteen perusteella, eikä teleoperaattorin tarvitse välttämättä olla näistä edes tietoinen, kunhan suostumus sijaintitiedon luovutukseen on saatu.

Pakottava sääntely?

Pakottavalla sääntelyllä tarkoitetaan tässä tilanteita, joissa lakisääteisesti kielletään paikannus tai paikkaperusteisten palveluiden hyödyntäminen edes käyttäjän nimenomaisella suostumuksella. Pakottava sääntely voi olla tarpeen heikomman osapuolen suojaamiseksi tietyissä tilanteissa, kuten työsuhteissa. Pakottavan sääntelyn täytyisi kuitenkin rajoittua välttämättömiin ja selkeisiin tapauksiin, sillä pääsääntöisesti käyttäjällä pitää olla oikeus määrätä oman sijaintitietonsa hyödyntämisestä. Tämä lähtökohta on tiedollisen itsemääräämisoikeuden mukainen. Pakottava sääntely on perusteltua tilanteissa, joissa pakottavalla sääntelyllä pyritään esim. varmistamaan käyttäjän todellinen itsemääräämisoikeus.

Työelämän ja tiettyjen muiden erityistilanteiden osalta on voimassa erityisnormistoa, joka sisältää pakottavaa sääntelyä. Kulloinkin sovellettavaksi tulevat erityisnormit tulee aina tutkia huolellisesti ennen seurannan mahdollistavan paikkaperusteiden palvelun käyttöönottoa.

Immateriaalioikeudet

Paikkaperusteisten palveluiden tarjoamisessa tullaan hyödyntämään paikkatietoja sisältäviä tietokantoja. Myös kartat muodostuvat usein käytännössä paikkatietoja sisältävistä tietokannoista. Tietokannat voivat nauttia oikeudellista suojaa, jos ne täyttävät tekijänoikeuslaissa säädetyt edellytykset. Tietokantojen suoja voi kannustaa uusien tietokantatuotteiden kaupallistamiseen, mutta toisaalta se voi johtaa tietokantoja hyödyntävien palveluiden kaupallistamisen vaikeutumiseen.

Tietokantojen suojan kriteerit ovat suojan uutuudesta johtuen vielä epämääräiset, ja siksi on vielä vaikeaa arvioida suojamuodon todellisia käytännön vaikutuksia.

Yksittäinen paikkatieto (koordinaattipari) ei yleensä yllä minkään tekijänoikeuslaissa säädetyn suojamuodon tasolle.

Sopimukset ja vastuukysymykset

Keskeisimmät paikkaperusteisiin palveluihin liittyvät kysymykset koskevat palvelua koskevan sopimuksen tekemistä. Sopimuksen tekeminen mobiililaitteella on usein vaikeaa ja vaadittavan tiedon esittäminen epäkäytännöllistä. Uudet EU:n direktiiveihin perustuvat tiedonantovelvoitteet voi olla vaikea täyttää, ja kohtuullista joustavuutta tulisi käyttää normiston tulokinnassa.

On helppoa kuvitella tilanteita, joissa paikkaperusteisen palvelun virheet johtavat huomattavaan vahinkoon. Vahingonkorvausvastuuta palveluiden tarjoajat voivat pyrkiä rajoittamaan informoimalla markkinointi- ja esittelyaineistossaan ja sopimuksissaan selkeästi palvelun saatavuuteen ja laatuun liittyvistä rajoitteista ja puutteista. Pelkät standardit vastuunrajoitusehdot käyttäjäsojimuksessa eivät välttämättä riitä, jos muun informaation perusteella käyttäjällä on ollut perusteita luottaa palvelun saatavuuteen tai laatuun.

Positioning technology: Current Regulatory Framework

Executive Summary

Applicable Law and Data Protection

The general law regulating the processing of personal data in Finland is Personal Data Act. If location data is personal data, the Personal Data Act is generally applied to the processing of such location data. As a general law, the Personal Data Act applies to processing of personal data unless otherwise provided elsewhere in the law. The Personal Data Act is partly based on the EU Data Protection Directive. Another important field of regulation is Tele Privacy Act based on Tele Privacy Directive. The Tele Privacy Act sets forth special provisions on data security and privacy in the field of telecommunications. Furthermore, in many other fields of regulation there are other norms concerning processing of personal data.

A new Tele Privacy directive has been enacted by the European Union as a part of a large regulative package concerning electronic communications networks. The new privacy directive changes the regulative framework considerably. The directive includes certain express provisions on location data. The exact interpretations of those provisions are still somewhat unclear. However, the directive will bring, when implemented, a welcomed clarification to the present situation. It has been predicted that the implementation of the directive will not take place in Finland before the year 2004. If this is actually the case, the industry will have to comply with the existing regulations for a considerable time. It could be in the interest of all parties that the present regulations would be interpreted, to the extent possible, within the context of the new directive in order to ease the transition.

Provisions of the new directive do not differ greatly from the general data protection regulations in the European Union. Indeed, the main purpose of the directive is to “particularise and complement”² the general Data Protection Directive with respect to the processing of personal

² Article 1, paragraph 2 of the Directive on privacy and electronic communications, 2002/58/EC

data in the electronic communication sector. The main differences concern (i) the allowed utilisation of the personal data (in the new directive only consent, under the general data protection regulations also other cases such as assignment, contract and relevant connection), (ii) detailed provisions on information to be made available to the users of such services, and (iii) user's right to temporarily refuse the processing. It has been questioned whether special regulation on processing of location data would be needed at all and whether the general data protection regulation would suffice. Taking into account of the sensitive nature of the data processed and the special characteristics of the field, it is the opinion of the author that special regulation is needed for ensuring the confidence of the consumers and for recognising the special regulative needs in the field of telecommunications.

There are differing views on the compulsory nature of the present Tele Privacy Act of Finland, but discretionary interpretation of the Act is only viable solution for the provision of location-based services. The adoption of the new directive will render this question obsolete.

Utilisation of Location Data

The different methods for generating location data can be generally divided into two basic categories as follows:

- Terminal-based positioning
- Network-based positioning

In case of terminal-based positioning most questions related to the role of the teleoperator are irrelevant: the user sends location data as a part of the contents of a message and teleoperator is merely providing ordinary communication service on an electronic communications network.

In network-based positioning there are several difficult questions relating to the role of the teleoperator or other controller of the network (as in most cases it is teleoperator that carries out the network-based positioning hereinafter only teleoperator's role is examined). For example, in what cases may the teleoperator generate and utilise the location data and in what cases he may deliver it to third parties?

Consent of the User

It is proposed in this report that that usually a sufficiently informed and conscious consent of the data subject is sufficient for processing of location data, and an order for a location-based service can constitute such consent, if processing of location data for the provision of the service is evident. Interpretation of this question can be important, since under the New Tele Privacy Directive an express consent is always required for processing of location data. It is recommended that the requirements for the consent in different situations are particularised in the implementation of the directive, and a possibility for implied consent would be allowed in cases where the processing of location data is evident from the context of the service.

The service can be constructed so as to clearly inform the user about the nature of the service. The method for provision of sufficient information and acquiring sufficient consent should be taken into account early when planning the services.

Services requiring continuous positioning involve certain special privacy risks. These risks can also be effectively curtailed with careful planning of the location-based service. It is possible that the differences between continuous positioning and instant positioning (as defined in Section 2.3) should be taken into account in the implementation of the directive.

Also services involving third-party positioning (monitoring service, defined in Section 2.3), involve special privacy risks, which should be taken into account when constructing the service. It should also be examined how to ensure that users are aware of the monitoring services set up for the mobile terminal. This could be achieved, for example, with periodic reminders to the mobile terminal about the on-going monitoring services.

Structures and processes adopted for the utilisation of location data are directly related to the market structure for location-based services. Flexible processing of location data should be always balanced with the related privacy issues so that the effective functioning of the market is enabled without prejudicing privacy of users.

Relationships of Teleoperator and Service Provider

In network-based positioning it will be necessary for the provider of location-based service to acquire location data from a teleoperator (or other party providing the positioning service). Thus Service Providers will have to comply with the legal and technical requirements set by Teleoperators for the delivery of the location data. Teleoperators will set the requirements on the basis of their customer-relationship with the user so that the Teleoperator ensures compliance with its own obligations with regard to the privacy of the user. There are several methods for the Teleoperator to ensure that the user has given a consent for the delivery of location data to the Service Provider.

It should suffice that the teleoperator has ensured the consent of the user for the delivery of the location data to the Service Provider. In other words, teleoperator should not be made liable for the processing of location data by a Service Provider. For example, ensuring a purpose-specific consent should not be an obligation of the teleoperator. The purpose of the processing of location data by the Service Provider (and by that the limits for the processing) is defined by the relationship of the Service Provider and the user, and it is not even necessary for the Teleoperator to be aware of that purpose.

Compulsory Regulations?

By compulsory regulation we mean regulations prohibiting utilisation of location data even with the express informed consent of the user. There are certain cases where compulsory regulations will be necessary. Cases where compulsory regulation would be in place are cases where the user is in a position that it would in practise be difficult for him/her to prohibit positioning or not to give his/hers consent for positioning. For example, employment relationships are such cases: it might be difficult for the employee not to give his/hers consent for the positioning by the employer. Also minors might in certain cases be in need for compulsory protection. In both these cases there are special regulations in place in Finland. Interpretations of those regulations differ from case to case. It should be analysed whether compulsory protection would be needed in some other fields with regard to monitoring services.

Generally compulsory regulations should be limited to situations where they are clearly necessary. On the basis of the principle of informational self-determination a user should have a

right to determine the use of his/hers personal data, including location data, and authorities should intervene only if necessary to ensure the actual self-determination.

There is always a risk that user's consent for a monitoring service is affected by his position with the user of the monitoring service. Thus the privacy risks cannot be prevented entirely.

Intellectual Property Rights

Databases produced by companies for the provision of location-based services are often protected as databases, which makes investments into the collection of such databases and offering of such services more viable. On the other hand, database protection complicates production of content services, as companies will have to ensure that they have the rights needed. Database protection may extent the protection in a surprising way.

The interpretation of the new database protection is cumbersome and it is difficult to forecast what are practical implications of the protection. It is probable that collectors and generators of different kinds of compilations of data, such as fixture lists, and other list relating to sports events will try to demand licenses for the utilisation of the data collected by them.

A single set of coordinates generated by the computer system or otherwise does not qualify for copyright protection. It is also probable that a single set of coordinates does not qualify for database protection: a single set of the co-ordinates as such does not form a database. Thus, a single set of spatial data as such is not protected by IPR at all and IPR does not set any limits for the utilisation of a single spatial data.

Contracts and liability issues

The main contractual questions relating to location-based services concern the conclusion of the contract between the provider of the service and the user. The conclusion of the contract with a mobile terminal is difficult and impractical. The new obligations based on EU directives, including the recently implemented e-commerce directive, on the information to be provided to the customer complicate the matter. Reasonable flexibility should be allowed in the

methods of providing the required information for mobile services, as the capabilities of mobile terminals are limited.

Utilisation of location data often involves navigation, transportation or traffic. It may also be used in emergency situations for different purposes. It is easy to foresee how a failure to provide a requested location data or location-based service, a mistake in provision of the service, or merely a low quality of the service may cause considerable damages. Thus the liability questions related to the provision of location-based services seem to be essential for Service Providers. In case of ordinary location-based services the liability can usually be effectively limited if in the service description, in the marketing material and in the service agreement the limitations in the quality and availability of the service are presented clearly.

Positioning technology: Current Regulatory Framework

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. According to the original project plan, 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.

(iv) 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. *Relevant fields of 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, regu-lative issues in certain important fields, such as direct marketing and employment relations, are analysed.

In short, the relevant questions analysed in the report are the following:

- The legal nature of location data
- Utilisation of location data
- Teleoperator's control over location data
- IPR protection of location data and spatial information
- Utilisation of public information resources in provision of location-based services

- Licensing of IPR for location-based services
- Liability questions pertaining to the provision of location-based services
- Concluding Agreements with mobile terminal
- Requirements set forth in the recent and future EU legislation
- Analysis of certain fields of utilisation of positioning technology, such as
 - Protection of privacy in employment relations
 - Positioning of persons under guardianship
 - Direct marketing with positioning technology

2.3. Classification of Location-based Services

Service Classifications

There are many ways to classify location-based services. Supporting project of the NAVI programme KEN (“Key Usability and Ethical Issues in the Navi Programme”) has produced a report on different ways to classify products and services for personal navigation. In the report different ways to classify location-based Services from the point of view of a user are presented. KEN proposes the following dimensions for classification:

1. User
2. User goal
3. Environment
4. Equipment
5. Service characteristics.

In the KEN report a classification proposed by Roger Granberg of MobilePosition is presented: division of location-based services into filter and finder services.

- Filter: information concerning a location
- Finder: information on a location of the user / other objects or users

In the filter services location data is utilised to specify in more detail the exact information needed by the user. By providing information relevant to the position of the user – infor-

mation filtered based on location data - information overload is prevented. On the other hand, in finder services location data is used to locate people and/or things that are relevant to the user. In finder services location data is not merely used for filtering information, but location data is part of the service provided.

For juridical analysis of location-based services a different kind of classification might be needed.

Classifications concerning the nature of the positioning

Classifier	Categories	
<i>Who is using the location-based service?</i>	The person being located (<i>self positioning</i>)	Another person (<i>monitoring</i>) - statutory monitoring - contractual monitoring
<i>How long does the positioning last?</i>	Only current location produced and deleted instantly (<i>Instant positioning</i>)	Location data produced continuously (<i>Continuous positioning</i>)
<i>Is location data stored?</i>	No (<i>non-stored location data</i>)	Yes (<i>stored location data</i>)
<i>Where is location data produced?</i>	In user's terminal (<i>handset-based positioning or terminal-based positioning</i>)	In teleoperator's data systems (<i>network-based positioning</i>)
<i>Is user identified?</i>	No (<i>anonymous positioning</i>)	Yes (<i>non-anonymous positioning</i>)
<i>Can positioning be denied?</i>	Yes (<i>non-mandatory positioning</i>)	No (<i>mandatory positioning</i>)
<i>Is positioning chargeable?</i>	No (<i>free positioning</i>)	Yes (<i>chargeable positioning</i>)

Classifications concerning the nature of the service

Classifier	Categories		
<i>Has the user ordered the service?</i>	Yes (<i>ordered service</i>)		No (<i>non-ordered service</i>)
<i>Is the service delivered based on user's individual or immediate request?</i>	Yes (<i>pull service</i>)		No (<i>Push service</i>)
<i>Is location data stored?</i>	No (<i>non-stored location data</i>)		Yes (<i>stored location data</i>)
<i>Is the service instant or continuous?</i>	<i>Instant service</i>		<i>Continuous Service</i>
<i>For which purpose is the service</i>	Filtering relevant	Finding location of	Navigation to a desired

<i>used?</i>	location-specific information	another person	destination
--------------	-------------------------------	----------------	-------------

The category *monitoring* is divided into subcategories *statutory monitoring* and *contractual monitoring*. It bears to mention that in practise statutory monitoring may be utilised mainly in relation to police investigations, emergency situations and other similar circumstances.

A very important division is that between *instant positioning* and *continuous positioning*, especially in case of location data being stored. Questions relating to continuous positioning will be examined in some sections of the report in detail.

Another important classification is on the production of location data: whether location data is produced in the terminal of the user or in the network, as this distinction can have an effect on the applicable law.

Classification of Actors

Various actors are involved in provision of location-based services. The following central actors are identified in the report:

Teleoperator	Provider of the telecommunications service
Service operator	Provider of the telecommunications services that does not have own network and is utilising a network of a teleoperator
Roaming operator	Provider of the telecommunications service offering telecommunications services to customers of other teleoperator
Location service provider	Provider of a service enabling positioning
Billing service provider	Provider of a service enabling payment of an service with a mobile terminal
Service provider	Provider of a location-based service (whether Filter service or Finder service)
User	User of the terminal that is being located
Requestor	Party requesting the delivery of location data
Authorizer	Party giving authorisation for delivery of location data

2.4. Concepts

The concepts concerning personal navigation are somewhat ambiguous. In order to clarify the usage of concepts, a separate project developing vocabulary of location-related concepts has been instituted. The vocabulary developed by the vocabulary-working group (sanastotyöryhmä) is available for the participants of the NAVI Programme.

3. *Different methods for generating Location Data in the Light of Data Protection Regulations*

3.1. Central Data Protection Legislation

The protection of personal data in Finland is based on the Finnish Constitution, according to which private life, honour and domestic peace of everybody shall be protected. Among the fundamental rights of the citizens is also a right for self-determination, based on which a person is, among other things, granted a right to control the use of his/her personal data. Finland has also entered into several international treaties, which include provisions on data protection, the most important ones being the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

The general law regulating the processing of personal data in Finland is Personal Data Act (523/1999) which came into force on June 1, 1999 and replaced the Personal Data Register Act. The Personal Data Act is applied to all processing of personal data. Under the Act personal data means any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household. If location data is personal data under as defined above, i.e. if location data is identifiable as concerning a private individual or the members of his/her family or household, the Personal Data Act is generally applied to the processing of location data. As a general law, the Personal Data Act applies to the processing of personal data unless otherwise provided elsewhere in the law. In many fields there is spe-

cial legislation on the processing of personal data. For example in health care regulation there are detailed provisions concerning processing of the personal data of a patient.

The EU directive 95/46/EC of the European parliament and of the council of 24 October 1995 sets forth the general legal framework for processing of personal data within the European Union (Data Protection Directive).

Another important field of regulation is the Act on the Protection of Privacy and Data Security in Telecommunications (Tele Privacy Act), which came in to force in Finland on July 1, 1999. The Tele Privacy Act sets forth special provisions on data security and privacy in the field of telecommunications. It sets forth certain special obligations for teleoperators (as defined in the Finnish Telemarketing Act). The relevant provisions of the Act are mainly based on the directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (Tele Privacy Directive).

Furthermore, in many fields of regulation there are other norms concerning processing of personal data in different fields, such as processing of personal data in health sector, protection of minors and persons under guardianship. Regulation in certain fields is analysed in Section 9.

A new Regulatory package titled "*a New Regulatory Framework for electronic communications infrastructure and associated services*" has been enacted by the European Union. The package includes a new directive for privacy protection in telecommunications and electronic communications in general (New Tele Privacy Directive). The directive includes detailed regulations concerning utilisation of location data and providing location-based services.

3.2. Methods for Generating Location Data

There are various methods for generating location data. In general, the most relevant technologies for this report are satellite-based positioning (i.e. GPS), and positioning based on mobile phone base stations.

The different methods for generating location data can be divided into two basic categories as follows:

- Terminal-based positioning
- Network-based positioning

Location data can be generated in the mobile terminal of a user. This is the case, for example in the satellite-based GPS-positioning. There are also hybrid technologies, where both tele-network and satellite navigation is needed for producing location data. In assisted satellite navigation certain information needed for satellite-based positioning is transmitted to the mobile phone from a base station, and the exact location data is then produced with satellite-based positioning. The assisted satellite navigation functions better in urban environment and indoor environment than a satellite-based navigation as such.

There are, in addition, other techniques to generate location data. Local positioning can be based on wireless local area network (WLAN), where the location is generated by a WLAN transmitter. Furthermore, there exists a technique where the mobile terminal determines its location on the basis of the known positions of the base stations utilising the signal of the base stations independently of the operators.

In case of a terminal-based positioning, location data is generated by the user's terminal equipment. This essentially means that location data is originally in the control of the user. Such terminal equipment could be, for example, a mobile phone with GPS-chip attached. One alternative for the prevalent future positioning technology is assisted GPS-positioning, where certain information needed in the positioning is delivered to the terminal via telecommunications network. Also location data generated with assisted GPS by the user's handset would be regarded as terminal-based positioning as location data would be in the sole control of the user.

In case of a network-based positioning, location data is generated by an entity offering location services. For example teleoperators are such service providers when utilising the telecommunications infrastructure in generating location data: location data is generated within the systems controlled by the networkoperator.

The distinction between terminal-based positioning and network-based positioning is important in, among other things, determining the applicable law regarding location data generated.

3.3. Location Data within the framework of the Tele Privacy Act

The communications between a mobile phone and a base station offer an effective and existing systems infrastructure for reliable and reasonably accurate positioning. It is likely that in many positioning solutions taken into use location data is generated within the teleinfrastructure of the teleoperator by the teleoperator (network-based positioning). Thus it is the teleoperator who has the first control to location data and it is the teleoperator that processes location data for offering the location-based services, for delivering location data to the customer or to a content service provider. Therefore provisions of the Tele Privacy Act, the data protection regulation of the field, may come to apply to the generating and processing of location data by teleoperators.

In the Tele Privacy Act (Section 3, item 5) “identification information” is defined as follows: the number of the subscription of a subscriber or user or other identification or *information created or stored in the course of making a call* (Finnish: *teleyhteyden toteuttamisessa*). If location data is perceived as identification information within the meaning of the Tele Privacy Act, a teleoperator has special obligations with regard to such data.

In the Tele Privacy Directive the corresponding norm is as follows:

Traffic data relating to subscribers and users *processed to establish calls and stored by the provider of a public telecommunications network...* must be erased or made anonymous upon termination of the call...

Hence, if location data is created or stored in *the course of making a call* (wording of the Tele Privacy Act), location data is identification information within the meaning of the Tele Privacy Act.

A reader is again reminded of the new Regulatory package of European Union coming into force in the near future, which will change the relevant EU regulations considerably. The effect of the renewal should be taken into account when developing new services or solutions.

3.4. Applicability of the Tele Privacy Act and the Personal Data Act

Above it is concluded that the provisions of the Tele Privacy Act concerning identification information are applied to information *created or stored in the course of making a call* (Finnish: teleyhteyden toteuttamisessa).

There have been differing views on the applicability of the Tele Privacy Act to location data, as it has been argued that the technical process through which location data is generated does not comply with the requirements of the Tele Privacy Act. That is, location data is not created or stored in the course of making a call or, within the wording of the Tele Privacy Directive; location data is not processed to establish calls. In spite of the wording of the directive, the definition of identification information in Tele Privacy Act (in Finnish: teleyhteyden toteuttamisessa syntynyt tai tallentunut tieto) clearly covers for example traffic data created in the course of SMS-messaging.

Turning back to the Tele Privacy Directive, the wording of the directive (establishment of calls) would suggest that the regulation is only applied in relation to phone calls. However, according to the Article 3 of the directive, it applies to the processing of personal data in connection with the provision of publicly available telecommunications services in public telecommunications networks. Telecommunications service is defined in the directive to mean services whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks, with the exception of radio- and television broadcasting. From this perspective it is evident that the applicability of the directive is meant to be broad.

It can be concluded that if location data has been generated or stored in direct connection to transmission of actual messages, be it voice or data, between a base station and a mobile phone, location data is identification data under the Tele Privacy Act.

What about other methods for generating location data? It is possible to generate location data on the basis of other radio signals transmitted between a base station and a mobile phone. Such signals are not related to any messages sent or received, and the user of the mobile phone need not be actively involved in transmission of these signals. Would location data generated in relation to this type of transmission be identification data under the Tele Privacy Act? From the wording of the Tele Privacy Act and the Tele Privacy Directive it could be concluded that this kind of location data would not be regulated under the Tele Privacy Act.

This kind of interpretation entails certain complications. First, it has probably not been the intention of the lawmaker to exclude certain information generated in relation to telecommunications from the applicability of the Tele Privacy Act. The purpose of the Tele Privacy Act and the Tele Privacy Directive has been to provide special privacy protection in the field of telecommunications. Excluding certain kind of location data, which can be deemed very sensible data, from the applicability of the regulation in the field merely on the basis of certain technical details would be counter to the goals of the regulation. In essence location data is, as far as protection of privacy is concerned, same kind of data as any other personal data processed by teleoperators in relation to telecommunications: it is personal data controlled by the teleoperator. Second, the proposed interpretation would lead to a situation where two different sets (Personal Data Act and Tele Privacy Act) of regulation would be applied to telecommunications services, which might complicate the regulatory framework, forcing teleoperators to analyse which set of regulation is applied to each piece of data. Third, the new directive on protection processing of personal data in the electronic communications sector will cover processing of all location data by the teleoperators.

It is the opinion of the author that the telecommunications regulation and the Tele Privacy Act is more suitable framework for regulating all location data generated or processed by the teleoperator within the teleinfrastructure. However, interpretation of the Tele Privacy Act and the technical processes involved in generating location data in different situations is not clear.

Mandatory or Discretionary Nature of the Tele Privacy Act

According to the Tele Privacy Act a teleoperator may utilise the identification information only for certain purposes. The Paragraph 9 of the Tele Privacy Act sets forth as follows:

Upon the termination of a call, a telecommunications operator shall erase or alter the identification information that has been created when establishing the call and stored by the telecommunications operator so that the parties to the telecommunications may not be identified unless otherwise provided for in this chapter.

Paragraph 10 of the said act provides for certain exceptions to the erasure obligation for the purposes of collecting the billing information needed.

Paragraph 11 of the Tele Privacy Act reads as follows:

Section 11

Processing of identification information in the marketing of telecommunications services

Upon the consent of the subscriber, a telecommunications operator may, during the period referred to in section 10, paragraph 2, process the identification information for the purpose of marketing its telecommunications services or its other services directly relating thereto in connection with the production of which the identification information has been created.

In short, according to the Section 11 of the Tele Privacy Act a subscriber may in the special cases give his consent to the use of the identification data also for other purposes than those set forth in the preceding Section. From the wording of the Section a question arises whether the Section is meant to be compulsory protection of the subscriber. The text of the Section 11 leaves the matter open to interpretations.

The legislative history does not include clear answer to the question. In relation to the section 9 of the Tele Privacy Act, the government proposal for Tele Privacy Act states as follows:

Myös joissakin telepalveluissa, esimerkiksi herätyspalvelussa tai jonotuspalvelussa, teleyritys voi joutua tallentamaan tunnistamistietoja, jotta se pystyy kokonaisuudessaan toteuttamaan käyttäjän *selkeän tahdonosoituksen mukaisesti haluan erityispalvelun*.

This comment suggests that the lawmaker is in the opinion that the regulation is non-mandatory and the user may give his consent to the processing of identification information.

Also the representatives of the Ministry of transport and communications have expressed their view that the Tele Privacy Act is not meant to be compulsory.

The supervisory authority in the field of telecommunications in Finland is the Telecommunications Administration Centre (TAC). Earlier TAC has adopted an interpretation that the data protection provisions of the Tele Privacy Act are not compulsory and a subscriber can give his consent to the use of the identification data also for purposes not prescribed in the Tele Privacy Act.

One of the general principles of data protection regulation in Finland is “right for self-determination with regard to personal data” (Finnish: tiedollinen itsemääräämisoikeus”). The same main principle is prevalent in the Data Protection Directive. The right for self-determination is also an integral part of the relevant international conventions such as the European Convention for the Protection of Human Rights and Fundamental Freedoms. The important role of the principle supports the discretionary interpretation, as mandatory interpretation would prevent a person from practising his right for self-determination in relation to location data.

Furthermore, it can be noted that the normal law-making practise in Finland is to expressly state a mandatory nature of a regulation. If a regulation is meant to be mandatory, that is usually clearly stated in the law and not left open to interpretation.

These arguments would support the interpretation that the provisions on processing of identification data would be non-mandatory.

Tele Privacy Directive does not take clear stand on the issue. The Article 6 of directive reads as follows.

Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network and/or publicly available telecommunications service must be erased or made anonymous upon termination of the call without prejudice to the provisions of paragraphs 2, 3 and 4.

The paragraphs 2, 3 and 4 include the same exceptions to the main rule than the Finnish Tele Privacy Act, such as billing information and for marketing with subscribers consent:

For the purpose of marketing its own telecommunications services, the provider of a publicly available telecommunications service may process the data referred to in paragraph 2, if the subscriber has given his consent.

In the recital 17 of the directive it stated as follows:

...whereas any further processing which the provider of the publicly available telecommunications services may want to perform for the marketing of its own telecommunications services may only be allowed if the subscriber has agreed to this on the basis of accurate and full information given by the provider of the publicly available telecommunications services about the types of further processing he intends to perform.

In short, the directive would allow both interpretations, mandatory and non-mandatory nature of the provision, but it somewhat favours the mandatory interpretation.

The European Commission has on July 12, 2000 published a proposal for a new directive on processing of personal data and protection of privacy in the electronic communications sector. In the explanatory memorandum of the proposal the Commission states:

A further change is made to Article 6.3 by creating a possibility for further processing of traffic data, not just billing data, for the purpose of value added services with the consent of the subscriber or user. With the extension of the data protection safeguards to traffic data generated by any transmission network for electronic communications, *the existing possibility for further processing of traffic data, limited to billing data and only for the direct marketing of the service providers electronic communications services, has become too narrow*. Today, value added services have been developed and can be offered based on particular traffic data and there is no reason to prohibit such services in cases where the subscriber has consented to the use of traffic data for the purpose of these services.

From this remark it can be concluded that the Commission interprets the protection as compulsory: the Commission states that the present possibilities for further processing of the traffic data have become too narrow, and that there is no reason to prohibit a subscriber from giving his consent to the processing of the traffic data for value added services. However, the proposal of the Commission for a new directive is not relevant material in the interpretation of the current legislation.

To recapitulate, there are differing opinions on the compulsory character of the subscriber protection in the Tele Privacy Act. The Act allows two interpretations, (i) that the protection under Section 10 is compulsory, and (ii) that the protection under the said Section is not compulsory and a subscriber can give his permission for the processing of identification information for other purposes. Compulsory Interpretation would render offering of the value added services based on location data impossible under the Tele Privacy Act, as the processing of the utilisation data for the purposes of providing such services would be in breach of the Act. As it will take some time before the new directive (see Section 8) will be accepted and implemented to member states' legislation, the Discretionary Interpretation would for practical reasons be the only viable solution. This interpretation is also supported by the general principles of European and Finnish data protection (self-determination), by the legislative history of the Tele Privacy Act, by opinions expressed by relevant authorities and by general law-making practise in Finland, as described above.

Later in this report it will be presupposed that the Tele Privacy Act is discretionary and user can give his consent to the processing of traffic data containing location data for provision of location-based services. From this presupposition it need to be considered what kind of consent of the user is sufficient for processing of location data. This question is examined in section 5.

3.5. Choice of Law

Choice of applicable law, the place of legal proceedings and enforceability of court orders have turned out to be extremely complex questions in the network economy, where several jurisdictions can be involved in a single transaction. Also in location-based services territories and legislations of many different countries may be involved and the questions about applicable law etc. become relevant.

In this report these complex and horizontal questions are not examined in detail at this stage. Only the choice of law relating to Data Protection is analysed shortly.

According to the Data Protection Directive national laws of a member state are applied if:

- (a) The processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State;
- (b) The controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

In short, country of origin applies within EU: the law of the country where the controller has an “establishment” is applied. If one controller has an establishment in several member states, laws of each of these member states are applied. The concept “controller” refers to the controller of the personal data, to the party determining the purposes and means of the processing of personal data. The same choice of law applies under the Tele Privacy Directive.

For example, in case of a German operator offering roaming services to a customer of a Finnish teleoperator not established in Germany, the controller is the Finnish teleoperator, and the Laws of Finland are applied to the processing of personal data by the Finnish teleoperator. In this kind of case, as described in more detail in Section 5.7, the German roaming operator is acting as a processor of personal data. The wording of the directive suggests, that the Finnish Personal Data Act would be applied also to the German roaming operator, as the controller is established in Finland, and the law of the country of the controller is applied.

There are cases when it is difficult to assess whether a controller has an establishment in a member state or not. The concept of an establishment under the Data Protection Directive clearly differs from the concept of establishment in other regulations, such as tax regulations, although this difference is not explicitly clarified in the directive.

It is worth noting that the European Data Protection regulations limits transfer of personal data to outside of European Union. However, it is explicitly stated that personal data may be transferred between EU-countries. This, in fact is one of the main goal of the harmonisation.

3.6. Conclusion: the Applicable Law in Generating Location Data

We have concluded that there are differing views regarding the applicability of the Tele Privacy Act for generating location data by a teleoperator. However, it is the opinion of the author that the most viable interpretation for the applicability would be as follows:

- Tele Privacy Act is applied when location data generated by the teleoperator within the teleinfrastructure;
- In all other cases Personal Data Act would be applied for generating location data, unless there is special regulations in a field that bypasses the Personal Data Act;
- The Personal Data Act is always applied as a general law also in cases where special regulations cover the generation of location data;
- In different fields a special regulations of that field are applied to the provision and utilisation of location-based services;
- The renewal of the Tele Privacy Directive will change the situation considerably: the new directive includes provisions on location data, which would be applied to all processing of location data, including processing by Service providers, and the provisions would cover also terminal-based positioning.

4. *Renewal of the European Regulations on Electronic Communications*

4.1. Background

European Commission has for long been preparing a set of directives for a new regulatory framework for electronic communications. The directive package was completed when the Directive on privacy and electronic communications was finally passed on 12 July 2002.

The goal of the package is to drive forward the liberalisation of telecommunications markets. The main emphasis of the package is thus on the regulation of the markets of electronic communications. The new Teleprivacy Directive replaces the existing Teleprivacy directive.

The directive package includes the following directives

- Directive (2002/21/EC) on a common regulatory framework for electronic communications networks and services
- Directive (2002/19/EC) on access to, and interconnection of, electronic communications networks and associated facilities
- Directive (2002/20/EC) on the authorisation of electronic communications networks and services
- Directive (2002/22/EC) on universal service and users' rights relating to electronic communications networks and services
- Directive (2002/20/EC) on the authorisation of electronic communications networks and services
- Directive on privacy and electronic communications (2002/58/EC).

The New Tele Privacy directive apply to the “processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community”. “Electronic communications service” is defined in the framework directive as services provided for remuneration which consist wholly or mainly in the transmission and routing of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but *excluding services providing, or exercising editorial control over, content transmitted using electronic communications networks and services*. The applicability of the directive does not extend to activities related to provision or production of content services. As will be described later, the applicability of the directive in certain cases and with respect to certain actors seem to be unclear.

It is expressly stated in the directive – as well as in the earlier Tele Privacy Directive in force – that that the provisions of the directive particularise and complement Data Privacy directive.

It is thus clear that Data Privacy directive is a general directive that can be used in interpretation of the Tele Privacy directive and in filling of the gaps of the directive.

Location data is defined in the directive to mean *any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service*. In the corresponding recital it is stated that *"location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time, to the time the location information was recorded"*.

The definition of location data in the directive can be understood to cover all kinds of location data irrespective of the method of determining the location and irrespective of the teleoperator's role in generating location data. The definition would cover, for example, location data generated by user's mobile equipment with GPS or other corresponding technology.

One of the purposes of the directive (defined in Article one) is to ensure an equivalent level of *protection of fundamental rights and freedoms*, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector in member states. This purpose, protection of fundamental right and freedoms, should be paid attention when interpreting the directive.

4.2. Regulations Concerning Traffic Data

The directive includes regulations concerning utilisation of Traffic data, which under the directive means *"any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof"*.

Article 6 Traffic data

1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3, 5 of this Article and Article 15(1).

2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.
3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.
4. The service provider must inform the subscriber or user of the types of traffic data which are processed and of the duration of such processing for the purposes mentioned in paragraph 2 and, prior to obtaining consent, for the purposes mentioned in paragraph 3.
5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

From the point of view of location-based services, the detailed regulations on traffic data include one major change compared to the earlier regulations: it is the explicit possibility to utilise traffic data to value added services, such as location-based services. The definition of traffic data can embrace information on the location of the user, such as cell-id or other corresponding information necessary for the communications and which indicates the location of the user.

From the wording of the article 6 it seems evident that the regulations are directed to providers of electronic communications services. It is explicitly stated in chapter three that “*the provider of a publicly available electronic communications service* may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services”. As noted above, the definition of publicly available electronic communications service expressly excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and services. It seems that most location-based services fall within this category and fall thus outside the scope of the definition of “electronic communications services, which is intended to cover the basic transmission and routing services. Traffic data transmitted to third parties, such as value added service providers, would not be un-

derstood to be traffic data under the definition of the directive, but would constitute other personal data. This interpretation is supported by the fact that in Article 9 (location data other than traffic data) value added service providers have been explicitly mentioned. This would entail that the utilisation of traffic data by value added service providers would not fall under article 6 but would be covered under the other data protection regulations, especially under the general Data Protection Directive and in Finland Personal Data Act. This would clarify the regulative framework for value added service providers.

The paragraph 3 of article 6 allows for providers of electronic communications services the utilisation of traffic data for provision of value added services. The paragraph does not mention transmission of traffic data to third party service providers, and paragraph 5 limits the processing of traffic data to “*persons acting under the authority of providers of the public communications networks and publicly available electronic communications services*”. As noted earlier, the definition of publicly available electronic communications services excludes services “*providing, or exercising editorial control over, content transmitted using electronic communications networks and services*”. As the definition of electronic communications services seems to exclude content services, it appears that traffic data should not be transmitted to the providers of content services if they are not acting under the authority of a provider of a publicly available electronic communications services. The question is thus, is Article 6 intended to allow transmission of traffic data to providers of value added services? This seems clearly to be the purpose of the law-maker. As we shall see later, the directive explicitly allows transmission of other location data to third party service providers, such regulations being more detailed and stringent in many other respects.

It is to be noted that Article 6 clearly allows utilisation and transmission of traffic data that has been made anonymous. This simplifies provision of basic location-based services where personalised traffic data need not be transmitted to third parties.

In the recital 15 of the new Tele Privacy directive it is stated as follows:

“...Any further processing of such [traffic] data which the provider of the publicly available electronic communications services may want to perform for the marketing of its own electronic communications services or for the provision of value added services, may only be allowed if the subscriber has agreed to this *on the basis of accurate and full information* ...about the types of further processing it intends to perform *and about the subscriber’s right not to give or to with-*

draw his consent to such processing. ...Service providers should always keep subscribers informed of the types of data they are processing and the purposes and duration for which this is done.

The recital emphasises teleoperator's obligation to inform the user on details of the processing of traffic data. Such full information would include information about subscriber's right to withdraw his consent to the processing of the personal data. This obligation is not expressly set forth in the actual provisions of the directive.

4.3. Location Data Processed within the Teleinfrastructure

The applicability of the new directive is somewhat ambiguous. It is possible, taking into consideration the purpose of the directive and the contents of the article 9, that the definition should be understood so as to cover location data processed within the electronic communications network as a location data: i.e. the definition should cover location data processed as a location data, and not location data that is merely transmitted via the network as a contents of a message. This would be in line also with the interpretation that the regulations concerning traffic data cover only processing of traffic data by providers of electronic communications services. It is the opinion of the author that this would be sensible interpretation. The definition could be clarified so as to include only processing of location data in an electronic communications network *as a location data*, and not location data merely distributed over an electronic communications network as a contents of a message. After this interpretation, the question is, what should be understood to constitute processing of location data within the electronic communications infrastructure.

It is evident from Article 9 that certain regulations of the article are to cover also processing of location data by providers of value added services.

The New Tele Privacy directive includes detailed and elaborate provision on processing of location data:

Article 9

Location data other than traffic data

1. Where location data other than traffic data, relating to users or subscribers of electronic communications networks or services can be processed, these data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.
2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.
3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the electronic communications network or service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

The directive would provide that location data might be processed only with user's consent to the extent necessary for provision of the service. The directive would obligate the service provider to inform the user on certain details of the service. As noted above, under the current regulation all such information need not always be explicitly provided. The obligation entails similar problems as information obligations in the Distance Selling Directive: delivery of the requested information is difficult, or at least very impractical, in the mobile environment due to the limitations of mobile terminals and data transfer capacity. These limitations of the mobile terminals should be taken into account when interpreting the directive and obligations concerning information obligations. In practise provision of all requested information to the mobile terminal of the user when providing the service will probably not be viable solution and other means for providing the information must be sought.

In the recital of the directive reference is made to the Data Privacy Directive in specifying the nature of the required consent:

"For the purposes of this Directive consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject's consent as defined and otherwise determined within Directive 95/46/EC."

As mentioned earlier, 'the data subject's consent' under the Data Protection Directive means freely given specific and informed indication of wishes of the data subject. The Personal Data Act states explicitly that the consent must be voluntary, detailed and conscious expression of will. The questions related to the nature of the consent required are discussed in section 5.4.

The directive would expressly permit processing of location data only with the consent of the user or subscriber, and not in any other situations. The Personal Data Act enables processing of personal data in many other situations, including assignment by the data subject and relevant connection. The meaning of this difference is analysed in Section 5.4. In short, it is argued that in practise (i) explicit consent and (ii) assignment or performance of a contract as prerequisites for processing of personal data set forth in the Personal Data Act do not differ much in provision of location-based services.

4.4. Location Data – Traffic Data

The Paragraph 3 of the Article 6 of the New Teleprivacy Directive sets forth the requirements of processing traffic data.

“For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time.”

The provisions concerning traffic data and location data are to large extent similar, but also considerable differences exists. Especially the requirements on information available to the user differ, requirements set for location data being somewhat more stringent.

What is the motivation in the distinction between “traffic data” and “location data other than traffic data”? As earlier noted, traffic data may include information indicating the location of

a user. Teleoperator can, with further processing of traffic data and other data available, generate more precise location data, such data being “location data other than traffic data “.The main distinction between “traffic data” and “location data other than traffic data” seems thus to be the fact the traffic data is data that the teleoperator has to process anyway for the conveyance of the communications, and location data other than traffic data” is needed only for value added services or other corresponding functions separate from the communications as such. From this point of view there are certain grounds for the distinction. However, it can be questioned whether separate regulations for location data would have been needed at all, or whether general regulations concerning utilisation of identifiable data would have sufficed.

It can also be questioned why same rules could not be applied to the utilisation location data for value-added services irrespective of the origins of the location data.

It bears to notice that there are no norms covering utilisation of traffic data consisting of location data by value-added service providers: Article 9 covers only location data other than traffic data, and article 6 does not seem to cover processing by the providers of value-added service providers.

4.5. Location Data Processed by Providers of Location-based Services

It is clearly the intention of the law-maker to include in the directive regulations concerning providers of value-added services utilising location data. It is somewhat unclear which provisions are intended to regulate activities of value added service providers and which not. The article 6 explicitly mentions providers of electronic communications services as the objects of regulation. In Article 9 the wording is more general “service provider”. This would suggest that Article 9 should cover both providers of electronic communications services as well as providers of value added services.

This implies that also the utilisation of location data generated with terminal-based positioning methods would fall under the directive if such data is processed by providers of value added services. On the other hand, many details and wordings in the directive suggest that the provisions on processing of location data would concern only processing of location data

within the electronic communications networks. For example the Article 9 on special provision concerning location data begins: “*Where electronic communications networks are capable of processing location data*”. The condition for the applicability of the article is the characteristics of the electronic communications network. This suggests that only processing of location data within the electronic communications networks would be relevant, and could be interpreted to suggest that only network-based positioning would be covered.

It is the opinion of the author that the applicability of the directive should be limited to the processing of location data in cases where the special characteristics of the electronic communications network are present. This would also simplify the division of responsibilities among the authorities – general data protection authorities (Data Protection ombudsman in Finland) and authorities supervising the electronics communications services. The Personal Data Act sufficiently protects the privacy in other fields.

What are then the special characteristics of the electronic communications infrastructure? Reference could be sought from the New Tele Privacy Directive. Recital (5) specifies the background of the directive and the need for the directive:

[D]igital networks have large capacities and possibilities for processing personal data, The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk.

Recital 7 further states:

In the case of public communications networks, specific legal, regulatory, and technical provisions should be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, *in particular with regard to the increasing capacity for automated storage and processing of data relating to subscribers and users.*

The special characteristics of electronic communications networks referred to in the directive seem to be large capacity and possibility for processing personal data, increasing capacity for automated storage and processing.

4.6. Distinction of a User and Subscriber

The directive provides that the consent of the *user or subscriber* is required for processing of location data. "User" is understood to refer to a natural person using the electronic communications service. Subscriber – user relationship would refer to, for example, a relationship between an employer and employee. This brings along difficult privacy questions discussed in more detail in Section 5.5. EU has been aware of these problems, and in the recitals of the directive it is stated as follows:

"Whether the consent to be obtained for the processing of personal data in view of providing a particular value added service must be that of the user or of the subscriber, will depend on the data to be processed and on the type of service to be provided and on whether it is technically, procedurally and contractually possible to distinguish the individual using an electronic communications service from the legal or natural person having subscribed to it."

In the recital it is conceded that the distinction between the user and subscriber is difficult and proper interpretation depends on the situation.

4.7. Obligations of Teleoperator or Value Added Service Provider?

It was mentioned above that Article 9 of the new Tele Privacy Directive concerns also providers of value added services utilising location data. Who should then be responsible for the obligations under the article? For example, who in the last resort is responsible for ensuring that the user or subscriber has been given required information and that the user or subscriber has the required means to deny processing of location data? This questions needs to be analysed in more detail.

4.8. Conclusion

In short, the directive brings a welcomed clarification to the present unclear regulative situation. It would also facilitates the development of pan-European location-based services, as regulative unclarities involved diminish.

Provisions of the directive do not differ much from the general data protection regulation in the European Union. The main differences concern the allowed usage of the personal data (in the new directive consent always required, under the general data protection also other certain cases can come into question), and detailed provisions on information to be made available to the users of such services. It has been questioned whether special regulation on processing of location data would be needed at all and whether the general data protection regulation would suffice. Taking into account of the sensitive nature of the data processed and the special characteristics of the field, special regulation is needed for ensuring the confidence of the consumers and for recognising the special regulative needs in the field of telecommunications. The purpose of the new Teleprivacy directive is, according to the explicit notion in Article 1 of the directive, to particularise and complement the Data Protection Directive.

5. *Utilisation and Processing of Location Data*

5.1. General Remarks

According to the Personal Data Act “personal data” means any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household.

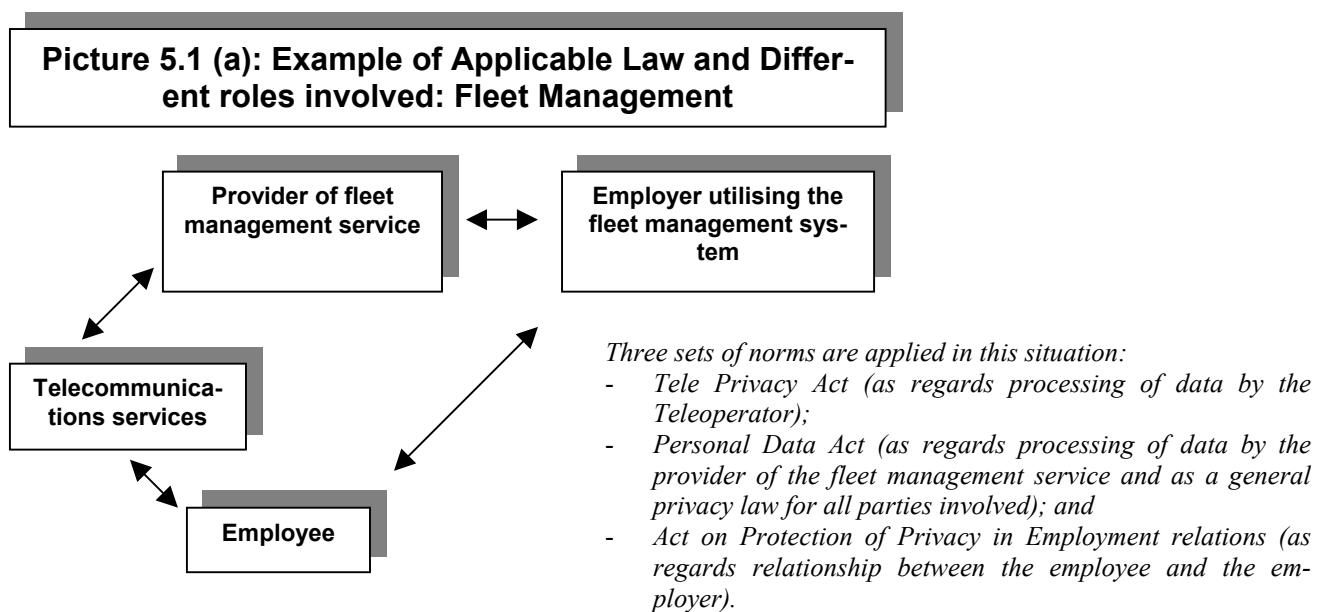
If a location data can be identified to concern a certain individual or the members of his/her family or household, the information is personal data within the meaning of the Personal Data Act. As a general law, the Personal Data Act is applied to the processing of personal data unless otherwise provided elsewhere in the Finnish legislation.

There are several methods for producing location data and it remains to be seen which technologies will become prevalent. Tele Privacy Act is applied only if location data is interpreted to be identification information as defined in the Act. As described above in section 3.2, choice of applicable law between the Tele Privacy Act and the Personal Data Act is difficult in certain situations. However, it is evident that Tele Privacy Act is not applied in case of a terminal-generated location data.

Again, it is to be noted that the Tele Privacy Act will be replaced or modified when the new Tele Privacy Directive will be implemented. According to the available information the implementation in Finland will take place in the spring 2004, the parliamentary elections causing a delay.

Applicable Law

The law applied to the processing of location data depend on the situation and on the roles of the parties involved. For example, in case of a fleet-management system, a teleoperator can have multiple roles: Teleoperator can process location data pertaining to a user employed by the teleoperator, transfer the data to a fleet management service provider owned by the teleoperator, which transmits the fleet management information needed to the teleoperators' fleet management unit. The situation would be as follows:

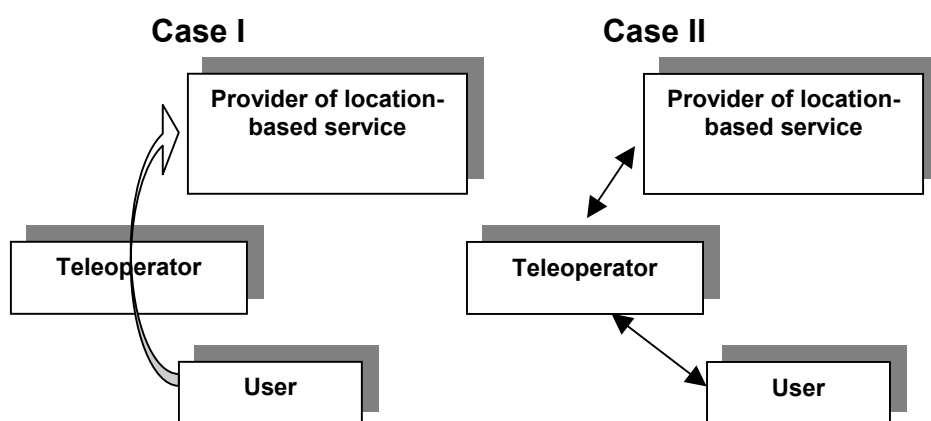


It is worth pointing out the limitations of the applicability of the Tele Privacy Act. A content of a message sent by a user of a mobile terminal is not regarded as traffic data in the meaning of the Tele Privacy Act. In case of a terminal-based positioning location data is usually transmitted to a service provider as part of a content of a message sent by a user. Processing of such location data by a teleoperator would not be processing of traffic data but general provi-

sions on the privacy of telecommunications. *Thus the provisions concerning traffic data in the Tele Privacy Act are applied to location data only if location data is processed by the teleoperator as a location data.* If location data is merely the contents of the message, the role of a teleoperator is merely the role of a transmitter of the message.

The picture below clarifies the situation:

Picture 5.1(b): Different Roles of Teleoperator and Applicable Law



Case I: user delivers location data generated with GPS systems to the service provider as contents of an SMS-message. Teleoperator transmits the message to the recipient without reviewing or knowing the contents of the message. The teleoperator acts merely as a transmitter.

Case II: user orders a location-based service. Network-based positioning is utilised. Teleoperator acquires the message, processes the information, retrieves location data and delivers information to the service provider. Location data is processed by the teleoperator.

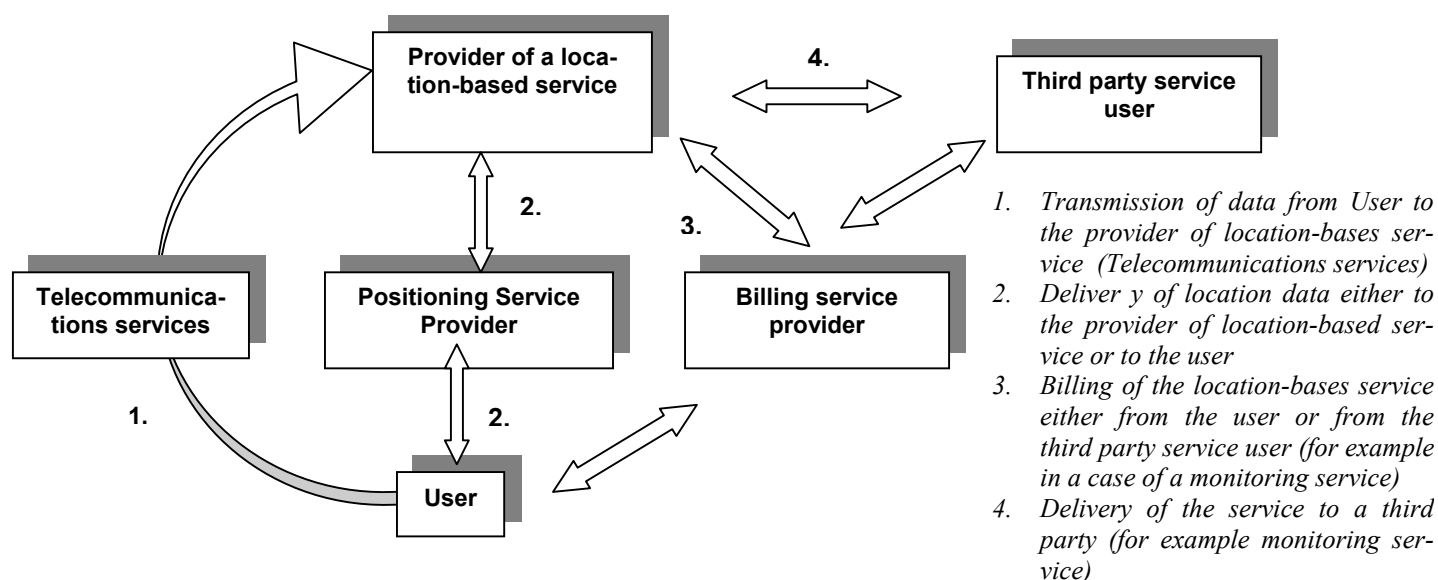
Role of a Teleoperator and a Service Provider

It should be kept in mind that due to the telecommunications regulations a teleoperator should separate its telecommunications services and other services such as content services or “Find a friend” type of services. This means that these services are offered in different business units.

For example, the Sonera’s location-based services under Sonera Pointer – trademark should not be offered by the teleoperator Sonera but by the content or service provider Sonera, which – on the basis of EU regulations – should be a separate business unit.

The structure should be as follows:

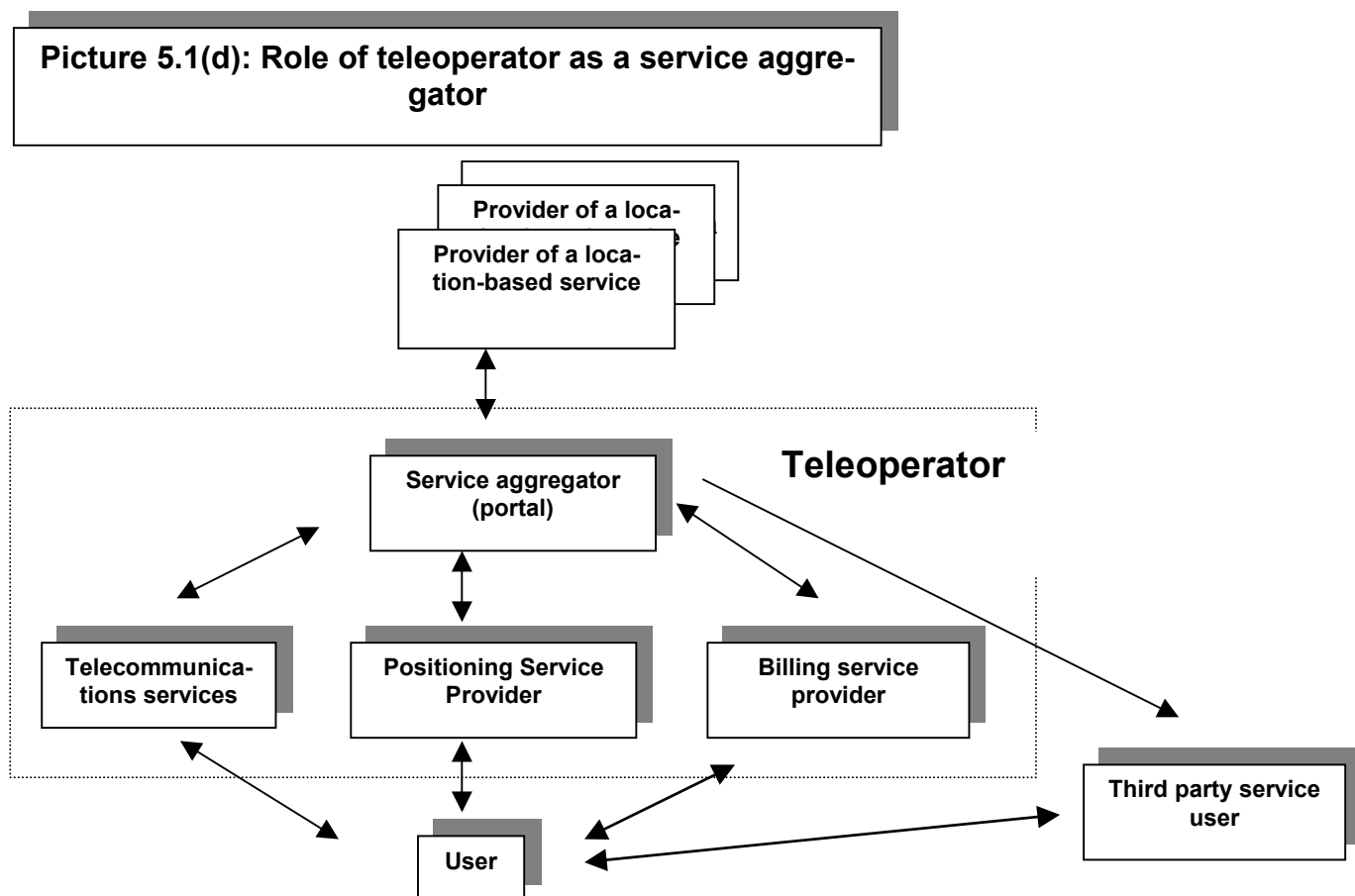
Picture 5.1 (c) Example of different actors and actions typically involved in provision of location-based services



In short, usually the service request is delivered to the Service Provider. The request is then delivered to the teleoperator for location data. The teleoperator delivers the data to the Service Provider, who then provides the service.

In practice the services provided at this stage in Finland are mainly at piloting stage and the above-described separation of businesses is not clear. Questions relating to the separation of business units are discussed in Section 5.7.

An alternative would be a structure where the service request is first delivered to teleoperator who then delivers the order to a third party service provider as described in picture 4.1(d) below. There are several reasons why this kind of a model could be more viable from the business perspective. It is possible that in practice this kind of a model will be prevalent.



In this kind of a market structure teleoperator is acting in several roles. This arrangement enables anonymous order for the service, as usually the identity of the user does not need to be revealed to the provider of a location-based service. Third party service user could be, for example, a user of a find-a-friend –service.

In this paper it is not assessed whether this kind of a business structure would be in accordance with the EU telecommunications regulations. Taking into account the purpose of the regulation, the role of the independent providers of location-based services and the openness of the interface offered by the teleoperator is probably relevant in the assessment. Generally the role of the service aggregator does not seem to be an integral part of provision of telecommunications services.

5.2. General Principles of the Personal Data Act

The Personal Data Act provides for general rules for processing of personal data, such as exclusivity of purpose (Section 7), necessity and accuracy requirements (Section 9). According to the exclusivity of purpose –principle personal data may not be processed in a manner incompatible with the pre-defined purpose. According to the necessity requirement only personal data that is necessary for the declared purpose may be processed. These principles are central to assessment of all processing of personal data.

According to the Section 24 of the Personal Data Act the processor of the personal data must see to that the data subject can have information, among other things, on the processor and on the purpose of the processing of the personal data. There will be no obligation to provide this information if the data subject already has relevant information. This is usually, albeit not always, the case when the initiative for processing of location data comes from the data subject himself. Therefore the information obligation is especially relevant in cases where the initiative for does not come from the data subject, such as cases based on relevant connection in accordance with the item 2 of the Section 8 of the Personal Data Act. It is worth to be mentioned that the information obligation under the Personal Data Act has only existed in Finland since summer 1999 when the Data Register Act was replaced by the new Personal Data Act. In several cases the fulfilment of the information obligation has proven to be difficult.

5.3. Prerequisites for Processing of Personal Data

The Section 8 of the Personal Data Act provides for the general prerequisites for processing of personal data. Personal data may be processed in following situations:

1. The data subject has unambiguously consented to the same;
2. The data subject has given an assignment for the same, or this is necessary in order to perform a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
3. Processing is necessary, in an individual case, in order to protect the vital interests of the data subject;

4. Processing is based on the provisions of an Act or it is necessary for compliance with a task or obligation to which the controller is bound by virtue of an Act or an order issued on the basis of an Act;
5. There is a relevant connection between the data subject and the operations of the controller, based on the data subject being a client or member of, or in the service of, the controller or on a comparable relationship between the two (connection requirement);
6. The data relate to the clients or employees of a group of companies or another comparable economic grouping, and they are processed within the said grouping;
7. Processing is necessary for purposes of payment traffic, computing or other comparable tasks undertaken on the assignment of the controller;
8. The matter concerns generally available data on the status, duties or performance of a person in a public corporation or business, and the data is processed in order to safeguard the rights and interests of the controller or a third party receiving the data; or
9. The Data Protection Board has issued permission for the same, as provided in section 43(1).

Personal data may, among other cases, be processed if the data subject has unambiguously consented to the processing. According to the Section 3 of the Act the consent must be a voluntary, detailed and conscious expression of will. The legal requirements for the consent are rather strict and detailed. The personal data may be processed within the scope of the consent received.

Second, processing of the personal data is allowed if the data subject has given an assignment for the same, or this is necessary in order to perform a contract to which the data subject is a party. This prerequisite could be fulfilled, for example, when a user has entered into a contract for providing a service based on processing of location data. Data Protection Directive does not mention assignment as a prerequisite for processing. However, entering into a contract can be understood also as an assignment for provision of the same.

Third, processing of personal data is allowed, if a connection requirement is fulfilled. Sufficient relevant connection would, according to the Act be, for example, clientship or membership. Based on the necessity requirement set forth in Section 9 of the Act, only data necessary for the declared purpose may be processed.

The employment relations and certain other special cases for processing of the data will be examined in more detail in Section 9.1.

In short, under the Personal Data Act personal data may be processed to the extent necessary for the intended purpose, if

- (i) User has given its unambiguous, voluntary, detailed and conscious consent for the processing;
- (ii) The user has given an assignment for processing of location data; or
- (iii) There is a relevant connection between the user and the processor of location data justifying the processing of location data.

Under regulations in certain fields, such as Tele Privacy Act, not all of the above mentioned rules apply.

5.4. Consent, Assignment and Relevant Connection

Consent

When the processing of location data is based on user's consent, the question arises, what is considered sufficient consent for processing of location data. In this chapter this question is pondered from the point of view of the Personal Data Act.

The Tele Privacy Act does not include any provisions on the nature of the consent.³ As a general law Personal Data Act is applied to processing of personal data to the extent not provided otherwise elsewhere in the law.⁴ Thus, provisions of the Personal Data Act can be applied in

³ In the Tele Privacy Directive it is provided that the consent of the subscriber for any further processing of data relating to the subscriber may only be allowed if the subscriber has agreed to this *on the basis of accurate and full information given* by the provider about the types of further processing he intends to perform.

⁴ The New Tele Privacy directive includes a recital where it is expressly stated that the consent is interpreted within the framework of the Data Protection directive

interpretation of the consent given by the user for processing of identification data also under the Tele Privacy Act.

According to the Personal Data Act the consent must be conscious. This entails, among other things, that the consent is not effective if it is hidden in the general terms and conditions of a service so the user does not have actual knowledge of the consent.

Consent must be also sufficiently detailed. The Data Protection Ombudsman has given statements where he has commented whether a consent given has been detailed. Would, for example, a general consent for processing of a location data given when concluding the service agreement with a teleoperator allow processing of location data? It is probable that such a consent would not be deemed detailed enough, as it would cover any processing of location data by the teleoperator.

What about a general consent given by the user to the teleoperator to process location data in connection to a service ordered by the user when location data is needed in connection to the provision of the service? Such consent could also be regarded too wide as the consent would not specify which services are within the consent and the consent would thus not be detailed enough.

An express consent would be, for example, a separate confirmation that the user gives his consent to the processing of location data on the basis of sufficient information about the nature of the service. Such separate confirmation would always satisfy the requirements of the Personal Data Act.

It can be concluded that a sufficiently detailed and express consent to the utilisation of location data given by a sufficiently informed user would satisfy the requirements of the Personal Data Act.

Assignment and a performance of a contract

It is somewhat unclear, what kind of an order for a service can be deemed as a sufficient assignment or a contract for processing of personal data. Personal data may be processed on the

basis of an assignment or a contract in accordance with the item 2 of Section 8 of the Act: the user gives an assignment for processing of the personal data. If the user orders a service for which processing of personal data is necessary, and it is evident from the context that location data must be processed for fulfilment of the order, the order for the service can be interpreted to fit within this provision. In such a situation the mere order of the service would suffice for processing of the personal data. The assignment resembles implied consent: the consent is supposed to be included in another expression of will of the user.

As mentioned earlier, the Data Privacy Directive mentions only a performance of a contract as a basis for processing of personal data. The distinction between an assignment and a contract is unclear, and in this paper it is assumed that there is no other relevant difference between them other than the fact that an assignment does not have to be an explicit contract.

For enabling processing of location data, contract entered into or the assignment given by the user must be of such nature that it inherently involves processing of location data. This means that the user should, on the basis of information available, be able to understand that the fulfilment of the assignment requires processing of personal data in certain extent. If this is not the case, the data subject has not given assignment to the processing of location data but for something else. If the need for processing of location data would not be necessary or not be evident in the context, order for a service would not include assignment for processing of location data, and a separate confirmation for processing of personal data would be required. From this point of view a need for a separate confirmation or consent for the processing of the personal data would depend on the information available to the user and the way the service has actually been presented to the user, not on utilisation of formal legal instruments such as description of the personal data file (rekisteriseloste).

This approach raises to the centre of attention the nature of the service and the way the service has been presented and explained to the user, and whether the user is aware of the utilisation of location data. This also lead to a conclusion that in practise explicit consent, an assignment and a contract might be closely similar as means for acquiring the authorisation for the processing of location data: in all these cases the information available to the data subject is decisive when determining whether processing of location data is allowed.

It can be concluded that an order of a service given by a user who has been sufficiently informed on the nature of the service and on the utilisation of location data in relation to the service could be regarded as an assignment or a contract in accordance with item two of Section 8 of the Personal Data Act and Article 7 item (b) of the Data Privacy Directive. It can also be concluded that in practise an assignment and a contract do not differ much from explicit consent given by the data subject, as in all these cases the information available to the data subject is decisive.

Relevant Connection

As mentioned earlier, personal data may be processed if there is a relevant connection between the processor of the personal data and the data subject. It is somewhat difficult to find examples where the relevant connection could be used as grounds for processing location data. This is due to the necessity principle of the Personal Data Act: not often would there be such a relevant connection between the processor and the data subject making it necessary to process location data. For example, a customership between a client and a teleoperator would not satisfy a necessity requirement.

One example where under the Personal Data Act the relevant connection could be established are employment relations: an employment relation could sometimes be a relevant connection justifying processing of location data in accordance with the necessity requirement. However, special regulation has been enacted in Finland for the protection of privacy in employment relations. Issues related to employment relations are handled in more detail in section 9.1.

It can also be argued that there is a relevant connection between a Service Provider and a user of a location-based service. In such cases processing of location data would be necessary for provision of the service, fulfilling the necessity requirement. However, in such cases the user must be sufficiently informed about the nature of the service so as to understand that he has order a location-based service. Therefore this kind of a relevant connection resembles often a consent given by the customer.

There will certainly be cases where the relevant connection can be used as grounds for processing location data. In such a case no express consent or assignment of the user would be

required. The extent of the processing of location data would be limited to the purpose and the data subject should be informed on the processing of location data as set forth in Section 24 of the Personal Data Act.

Conclusion

It can be concluded that in all cases the interpretation seems to boil down to the question how the user has been informed on the nature of the service and on the need for processing of location data. It can also be concluded that an order for a location-based service by a sufficiently informed user can be interpreted to enable the processing of location data. In short, *if user gives an assignment clearly aware of the utilisation of location data in relation to the assignment, this can be interpreted to be also a sufficient consent for utilisation of location data.* Validity of this interpretation can be important, if under the New Tele Privacy Directive an express consent is required always. Please refer to Section 4 for details on the renewal of the Tele Privacy Directive. This question is studied in more detail in the following Section.

5.5. Consent for Processing of Location Data by a Service Provider

Sufficient Consent?

It was concluded above that the nature of the required consent under the Personal Data Act is a decisive factor as the new Tele Privacy directive only acknowledges consent as a prerequisite for processing of location data, and the provision concerning consent in the general Data Protection directive and in the Personal Data Act are used in the assessment (both the new and the old Teleprivacy directive include an express reference to the definition of consent in Data Protection Directive).

The consent for the processing of location data can be given on case-by-case basis when ordering a service utilising location data.

A typical use-case would be as follows: A user needs a map of his location in Helsinki and sends an order for a map with his mobile apparatus. Would such an

order as such be deemed sufficient consent or should the service ask for confirmation for the use of location data?

In practise, acquiring an unambiguous consent in accordance with the requirements of the Personal Data Act would prove to be difficult and impractical. It is difficult to argue that a mere order of a service would include an unambiguous, detailed and conscious expression of will for processing of personal data. On the other hand, asking for a separate confirmation would also be impractical and would require at least two extra messages to be transmitted between the operator and the user. It is likely that in the long run users would find the separate confirmations unnecessary and annoying.

Based on Sections 5.3 and 5.4 it can be argued that usually *a sufficiently informed and conscious consent of the data subject is sufficient for processing of location data, and an order for a location-based service can constitute the consent*. There are some exceptions to this rule, as in certain fields compulsory protection is granted to data subject not allowing even voluntary processing of personal data. For example, employees and minors are granted compulsory protection against processing of personal data. These matters are looked in more detail in section 9.

For purposes of this section it is postulated that a sufficiently informed and conscious consent of the data subject is sufficient for processing of location data, and an express order for a location-based service can constitute such consent. How should the user be informed on the nature of the service?

Provision of Sufficient Information

There are many service types where the very nature of the service is to provide information or services on the basis of the location of the user. For example, a service where a mere location (coordinates) of the user is requested, it is evident from the context that location data will be processed in providing the service.

Often it might not be evident for consumers that a service requires processing of location data even if this actually would be the case. It is likely that when more location-based Filter services emerge and location data becomes merely one piece of information among the other

specifying the delivered content. In such a situation it would be very difficult to know which services utilise location data.

One way to provide the user with sufficient information on the processing of location data would be to collect all services utilising location data into a same group, for example, into a same sub-menu of a WAP-service. Alternative would be to take into use a symbol that would symbolise services utilising location data. For example, when ordering a location-based service through a WAP-phone, the menu item on the screen of the mobile phone would include a symbol that would mean that location data would be used for the service. It is likely that both these methods would provide the user with sufficient information in the light of the data protection regulation.

There are certainly also other methods that could be used for informing the user on the processing of the personal data. For example, if marketing information and other information available to the user includes sufficient notice on the utilisation of location data, user has ordered the service on the basis of the available information and thus should be aware of the utilisation of location data. Whether this would be interpreted as a sufficient consent depends on situation.

Example: in Sonera Pointer, no separate confirmation for the use of location data is required. Evidently it is supposed that the users of the service understand, on the basis of the marketing and other information available, that the provision of the service necessarily involves processing of location data.

It bears to mention that a subscriber of a mobile phone, who has the contractual relationship with the teleoperator, and the actual user of the phone may be different. Therefore the identification information may not always identify the actual user of a phone. Thus, location data should sometimes be understood to refer to a position of a mobile phone of the subscriber, not to a position of the user. If the identity of the actual user is not known by the teleoperator, no personal data concerning the user is processed, but the identification information refers to the subscriber. These issues have been taken into account in the new Tele Privacy Directive (See Section 4). For the sake of convenience, the term “user” is used in this section to refer to the user of the mobile phone irrespective whether this is the subscriber of the phone. Furthermore, it is supposed that in case the subscriber and the user are not the same persons and the identity of the user is not known by the teleoperator, the subscriber has authorised the user to use and

manage the mobile phone, and on behalf of the subscriber to give his consent for processing of location data pertaining to the subscriber. Whether this presupposition is sustainable will be examined later. It should also be noted that this is relevant mainly in cases of continuous positioning.

5.6. Special Cases: Continuous Positioning and Monitoring

Continuous Positioning

In instant positioning the user is positioned instantly on the basis of an order of the user. A far more complicated is a situation where a person subscribes to a service where positioning can take place several times over a longer period of time. In this report this kind of a positioning is called *continuous positioning* and a service utilising continuous positioning *continuous service*. The service can be used by the user him self or by a third party, and it is also possible that, after the service has been initiated, that third party can has a right to acquire and utilise location data of the user without each time obtaining a separate express consent from the user. Indeed, services based on continuous positioning are likely to yield most effective location-based services. Continuous positioning is necessary, for example, in so called Find-a-friend – services and in different kinds of fleet management systems. Also different kinds of navigation services will likely involve continuous positioning.

A typical find-a-friend –service is a service, where a group of users subscribe to a service where members of the group are allowed to acquire the position of another person in the group.

Fleet management –systems are utilised to manage resources of an enterprise, be it taxis, trucks or maintenance personnel.

Another example of a service requiring continuous positioning would be a service where the user has ordered location-specific information every time he arrives to a new town. The service provider should be able to monitor the location of the user and send the required information every time the user has arrived into a new town.

In this kind services the privacy risks involved are higher. Despite the privacy risks involved it should also be pointed out that services requiring continuous positioning can be highly effective and user-friendly services. If a user is aware of the nature of the service and is willing

to accept continuous positioning, there is no need for compulsory protection prohibiting these services.

At least the following privacy issues are relevant:

1. *Sufficiency of privacy information*: the user might not always realise the nature of the service requiring continuous positioning when ordering the service;
2. *Unauthorised positioning*: a third person having access to the mobile terminal of a user can initiate a service without authorisation of the user enabling monitoring of the user by that third party without the knowledge of the user;
3. *Invisibility of services*: as continuous services are not necessarily in any way visible to the user, it is possible that a person is not be aware of services he has subscribed to and thus would not be aware of the continuous positioning.

In all of the aforementioned cases the problem boils back to the question whether the user has acquired sufficient information on the service: in case (1) the question is about the information available to the user when ordering the continuous service. In cases (2) and (3) the question is about the information given or available to the user when the continuous service is on.

In order to overcome privacy issues raised here, the following methods could be used:

1. Ensuring that the user acquires sufficient information on the nature of service when subscribing to the service;
2. A separate reminder about the continuous service or continuous positioning delivered to the user's mobile terminal regularly.

A practicable way to ensure that the user acquires sufficient information would be to require a separate and express confirmation for services utilising continuous positioning. Such confirmation request would include a short description of the service requiring continuous positioning. It can be argued that this kind of an extra confirmation would not be too difficult procedure taking into account the nature of the service.

A continuous service requires continuous informing. If the user is reminded about the service regularly, the problems (2) and (3) above can be avoided or to the least curtailed: if a third

person has subscribed to the service with a user's mobile terminal, the user will become aware of the service through this kind of reminder. If the user has forgot about a service he has ordered earlier, a reminder will bring the service to his attention.

The reminder could be carried out in two different ways: (i) the Service provider sends reminder about the service; or (ii) the teleoperator sends a reminder about all such services to which location data is being delivered. It is the opinion of the author that the alternative (ii) would be a practical and clear solution to the problem in network-based positioning: the teleoperator may deliver location data only to such third parties (usually Service providers) that have been authorised by the user to receive such data. By informing the user about the recipients of location data the teleoperator also cuts down the risk of abuse of location-based services by Service providers.

A major Finnish telecommunications company has taken the following stand on the distinction between instant positioning and continuous positioning:

- Instant positioning: implied consent related to the service order sufficient;
- Continuous positioning: only an express and written consent sufficient.

Formalities such as a consent given in writing might not be necessary for continuous positioning. However it is evident that in case of a continuous positioning more detailed consent and process could be justified. A separate and express confirmation for subscribing to a service and a regular reminder about the service could be one solution.

Monitoring

In monitoring services the party utilising the service is not the user the mobile terminal but a third party that is monitoring the location of the user (such party hereinafter called "monitor"). These services usually involve continuous positioning. In short, many of the fears associated with positioning services relate to third party monitoring.

Once again, it is clear in this kind services the privacy risks involved are high. However, if a user is aware of the nature of the service and is genuinely willing to accept monitoring by a

certain third person, there is no need for compulsory protection prohibiting monitoring services. However, many cases can be identified where the monitored person is in such a situation where it would be difficult to deny monitoring. In these cases it should be pondered whether compulsory protection might be needed to protect the privacy of the users. Examples of these cases could be (i) employment relations (see in more detail Section 9.1), minors and persons under guardianship (see in more detail Section 9.4). Certainly other corresponding groups can be identified.

The question about the protection of weaker side in monitoring services is one of very high importance. However, in this report this partly ethical and also political question cannot be analysed further.

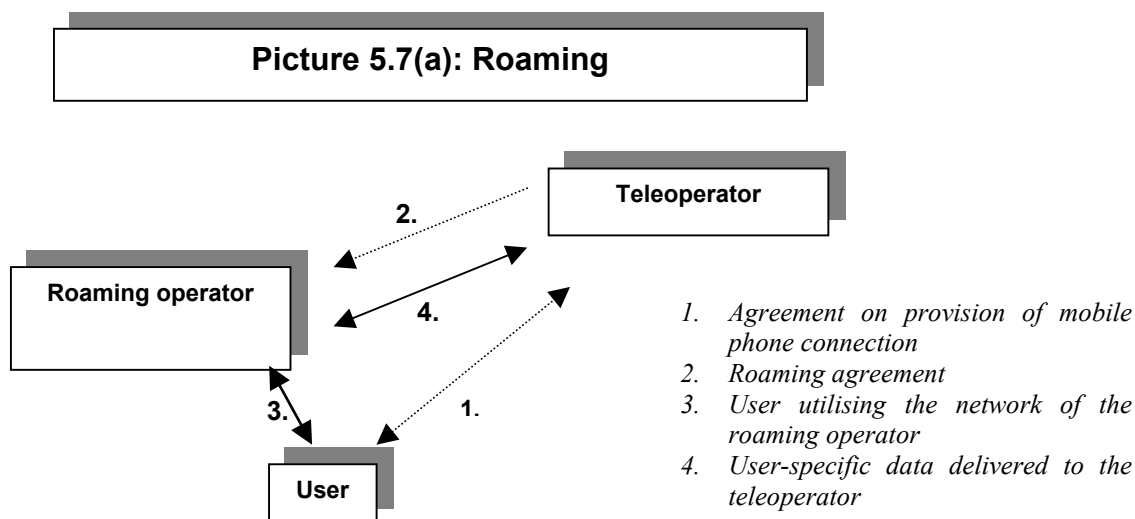
5.7. Transfer of Location Data Between Teleoperators

Transfer of identification information between teleoperators is central for the functioning of the telecommunications network. For example, roaming and operations of service operators not having their own network infrastructure could prove to be impossible without a transfer of such data.

In this section the basic questions pertaining to the transfer of identification information between teleoperators are examined.

In this chapter the following postulations are made: only processing of identification information within the meaning of the Tele Privacy Act is examined. Furthermore, in this chapter it is postulated that the teleoperator having the actual contractual relationship with the user has a valid right to process the identification information. The question is, how other teleoperators may process such data.

Roaming



One of the central technical characteristics of the modern mobile telecommunication system is roaming. Roaming makes it possible for a mobile phone to operate also in areas where the teleoperator does not have own mobile network, especially abroad. It is essential for the effective provision of location-based services that the location-based services are available also outside the network of the “home operator”.

A user case describing the present situation:

A Finnish mobile phone user is in Hanover. His mobile phone operates on the basis of roaming agreement between Deutsche Telekom and a Finnish teleoperator.

There is no agreement on provision of telecommunications services between the user and Deutsche Telekom. Deutsche Telekom’s (hereinafter DT) right to process and deliver the identification information is based on its agreement with the Finnish teleoperator, and DT is in fact acting on behalf of the Finnish operator, as a representative of the Finnish operator. Within the framework of the European Data Protection legislation, DT is the processor and the Finnish teleoperator the controller of the personal data.

A related user case: The Finnish teleoperator offers a service where maps of all cities of Europe are available on the basis of the location of the user. The user wishes to look at the map of Hanover. The order is sent to the Finnish teleopera-

tor, who inquires the location of the user from DT, and delivers the map needed on the basis of location data delivered by DT.

In this case again, DT is operating on behalf of the Finnish operator as the processor of the personal data. DT's right to process identification data of the user derives from its agreement with the Finnish teleoperator. Due to this arrangement the DT is also entitled to process location data of the user, and to transfer location data to the Finnish operator. As a "subcontractor" of the Finnish teleoperator, DT will not require confirmation of the user for the transfer of location data, as it is the responsibility of the Finnish operator to ensure that all necessary authorisations have been received.

The situation of DT can be compared to a company providing data processing services for technical maintenance of a customer register of another company. The controller (as defined in the Personal Data Act) of the data register is the company whose customer register is being processed, and the company offering the technical processing service does not have to check from registered persons whether the other company has a right to process the data, as it is the controller who is responsible.

The situation is in accordance with Section 8.1 item 7 of the Personal Data Act, according to which data may be processed if it is necessary for purposes of payment traffic, computing or other comparable tasks undertaken on the assignment of the controller. It is stated in the proposal of the government for the Personal Data Act that the provision is included merely for the sake of clarity, and the assignee would have the rights to process the data even without explicit authorisation in the Act.

The Data Privacy Directive includes corresponding and more detailed provisions on the relationships between the controller and the processor of the personal data.

Service Operator

The position of a service operator is somewhat similar to that of an operator utilising a network of another teleoperator for roaming. The service operator does not have its own data network, but has rented network connections from teleoperators and offers networks services to end-users under its own name. The user has entered into an agreement with the service pro-

vider. However, the teleoperator whose network actually is utilised for the provision of the network services is also processing personal data of the user. The teleoperator is allowed to do this on the same grounds as the roaming operator as described above, on the basis of an assignment in accordance with Section 8.1 item 7 of the Personal Data Act.

A system where each operator processing the identification information or personal data should ensure their right to process the data from the user would be extremely difficult to implement.

Conclusion

Within the framework of the European Data Protection legislation, a teleoperator utilising the services of another teleoperator is the controller of the personal data, the other teleoperator being the processor of the same.

Above we have concluded that teleoperator's right to process identification data or personal data is based on the original contractual relationship between the customer and a teleoperator, and other teleoperators' – such as in a case of roaming services or in relation between a teleoperator and a service operator - right to process such data is based on that relationship, other teleoperators acting as a “subcontractors”, processors of the personal data.

5.8. Transfer of Location Data between a Teleoperator and a Service Provider

In this chapter it is examined in what cases and under what preconditions a teleoperator is allowed to transfer location data to a Service provider.

In the preceding chapters it has been concluded that the following issues are uncertain: (i) whether Tele Privacy Act or Personal Data Act is applied to the processing of location data by a teleoperator; (ii) if Tele Privacy Act is applied, whether a use can give his consent to the processing of location data for the provision of location-based services.

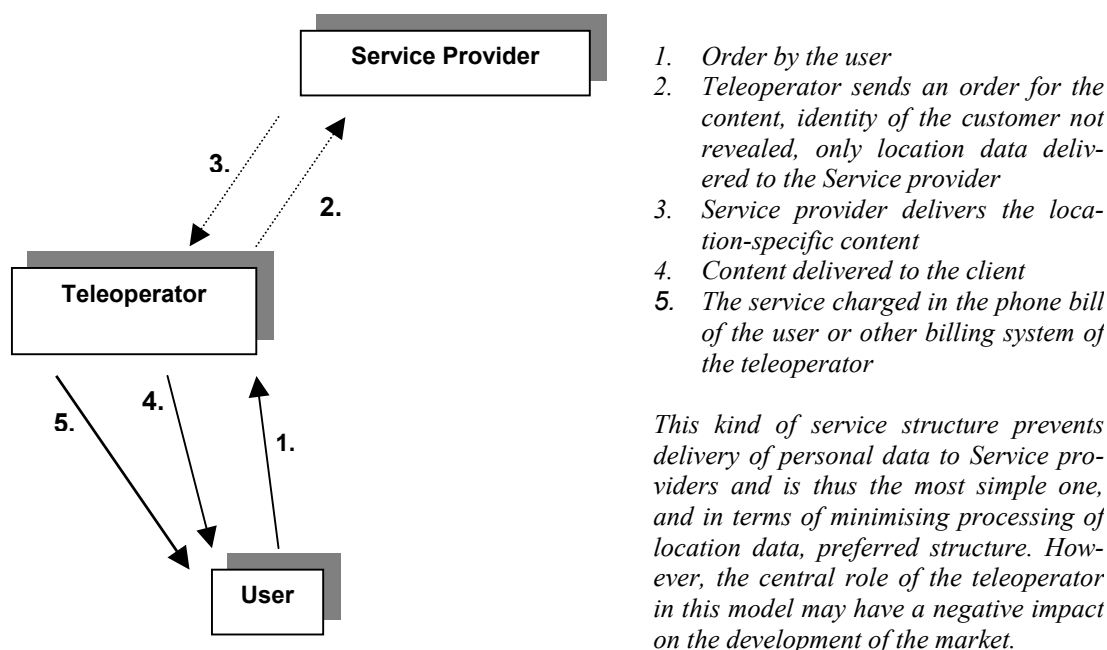
In this chapter it is supposed that the user may give his consent to the user of location data. This is practicable supposition, as the question relating to the compulsory nature of the Tele Privacy Act will become obsolete when the new Tele Privacy Directive is adopted.

As the Tele Privacy Act does not include regulation on transfer of the identification information, the rules of the Personal Data Act as a general law are applied.

Many teleoperators have extensive and separate content service departments. Generally, the position of an independent Service provider and a Service provider of a teleoperator is similar: to the extent teleoperator acts as a provider of telecommunications services, this activity is separated from other business activities, such as production of content services. The regulation on telecommunications mainly covers the activities of a teleoperator in offering telecommunications services. For example, the obligations on identification information concern only provision of telecommunications services. To the extent teleoperator is acting as a Service provider; Personal Data Act is applied to the utilisation personal data. This distinction is expected to change when the new Tele Privacy Directive is enacted.

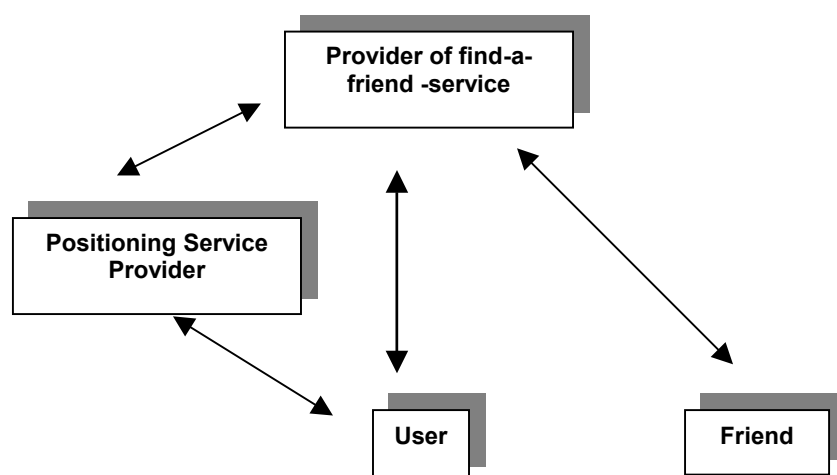
Case I: User is the customer of the teleoperator

Picture 5.8(a) Scenario 1: Teleoperator centered system



It is underlined that although the presented business structure seems to correspond to the present situation, the teleoperator should separate its telecommunications services from its content and other value-added services. Thus this market structure is not exactly in accordance with the telecommunications regulations of EU. In the light of the telecommunications regulations the teleoperator in the picture consists of (i) the telecommunications services unit (ii) the value-added-services-unit, as presented in the following exemplary model of relationships in provision of a find-a-friend service. (See also Picture 5.1 (d) for a detailed example of different roles of the teleoperator).

Picture 5.8(b): Model of a find-a-friend -service with network-based positioning



- *User authorises a friend to use the service;*
- *Friend sends a request for a location data of the User to be delivered;*
- *Service provider delivers the location data after having ensured that the Friend is entitled to acquire the location data*
- *Contractual relationship between the user and the friend not always necessary.*

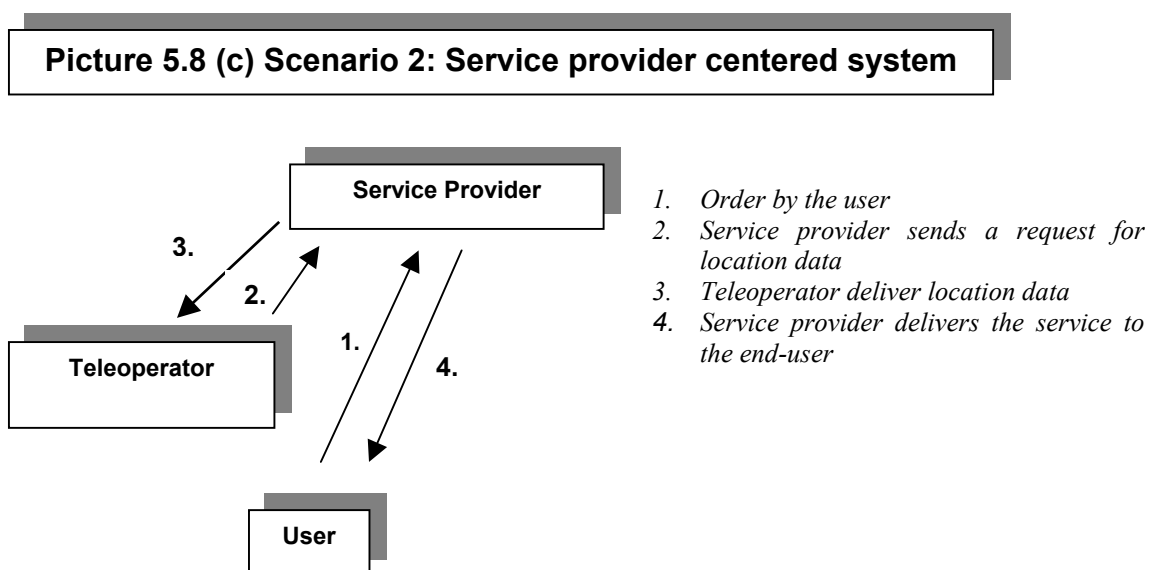
The starting point in the Personal Data Act is that the processing of personal data is allowed only if any of the prerequisites in Section 8 are fulfilled, and the data may be processed only in a manner compatible with the purpose of the processing.

It should be kept in mind that in cases where the customer relationship is between the teleoperator and the customer, and the service is charged by the teleoperator, transfer of personal data to the Service provider is usually not necessary: in most cases merely a delivery of anonymous location data is sufficient for the provision of the service. The Data Protection Ombudsman has expressed his opinion that to the extent processing of personal data is not

necessary for provision of a service (for example an online-news service), it should not be processed. From this point of view, transfer of personal data to Service providers in above-mentioned situations is questionable. Therefore it would be recommendable when developing technology and interfaces for location-based services to implement technology that allows delivery of anonymous location data to the provider of location-based service.

According to the Data Protection Ombudsman the user's consent may not override the necessity requirement set forth in Section 9 of the Personal Data Act. It can be asked whether a user can give his consent for transfer of processing of the personal data if that is not reasonably needed for the provision of the location-based service. It is possible, that such consent would be deemed not to be in accordance with the requirements of the Personal Data Act.

Case II: User is the customer of the Service provider



The legal issues faced in cases where the customer is directly the customer of the Service provider are somewhat different from those in other cases. This situation could come about in a situation where the user orders the location-based service for example with a SMS message directly from the Service provider.

The relevant question then is, how will the Service provider be able to acquire location data of the user. As described above, this problem comes about only if location data is not generated by the mobile apparatus of a user, but by the teleoperator. If location data is generated by the

mobile apparatus of the user, the user can deliver location data to the Service provider along with the order.

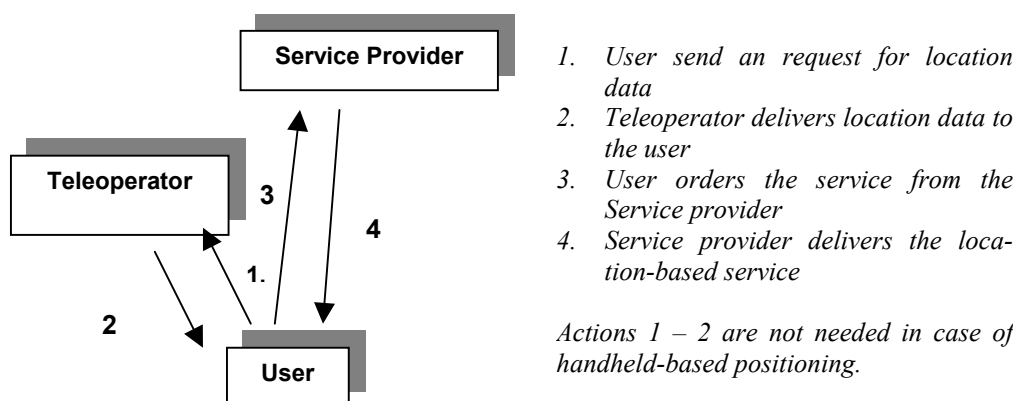
The situation is different if location data is generated by the teleoperator, in which case location data must be transferred from the teleoperator to the Service provider. The request for the delivery of location data can come either from the user or from the service provider. Direct authorisation of the user to the teleoperator would be impractical and would possibly render Service provider –centered model inoperative, unless the authorisation could be automated. Alternative is that teleoperator delivers location data on the basis of the request by the Service provider. In that kind of a situation the teleoperator should rely solely on the request of the Service provider. In case Service provider would in fact not have consent of the user for the utilisation of location data, delivery of location data by the teleoperator to such an unauthorised party would apparently constitute an infringement of data protection regulations.

Thus, it seems that the central question in a Service Provider –centered model is, *when the teleoperator can deliver location data on the basis of the request of the Service provider without direct authorisation of the User*. That is, how could the teleoperator ensure in this kind of situations that it is not violating data protection regulations? There are several alternatives, such as automated authorisations of the user or corresponding technical measures. Another alternative would be a market structure where the user would choose “trusted service providers” who could request location data from the teleoperator.

It should also be noted that a delivery of location data requires interconnection of data system of the Service provider to that of the teleoperator. This makes an agreement between the Service provider and the teleoperator necessary. In this kind of an agreement the framework for the delivery of location data could be agreed on. However, the question remains, How does the Service provider certify that it has a right to acquire location data and what would be sufficient proof of the right of the Service provider right to process the personal data? In practise there are several alternatives for ensuring User’s consent. In the steering group of the project different methods have been discussed.

Case III: User-centered system

Picture 5.8(d) Scenario 3: User centered system



This system would be clear from the legal perspective: the user acquires location data from the teleoperator or location data is generated by the user's handheld. Then the user sends location data along with other information needed for the provision of the ordered service. In case of handheld-based positioning this is the market structure.

In case of network-based positioning it is somewhat unlikely that this market structure will evolve unless the delivery of location data from the network to the user's terminal can be automated. In fact the delivery of location data has already been automated by a Japanese teleoperator: a base station of that teleoperator delivers automatically as a push service location data of the base station to all terminals within the reach of that base station. As the base station network is very dense in Japan, the accuracy of location data is sufficient for many services.

5.9. Internal Processing of Location Data by the Teleoperator or Service Provider

When the Service provider has received location data of the user, Service provider may process location data and other personal data only in accordance with the provisions of the Personal Data Act. As mentioned above, Personal Data Act provides for several norms, which

must be obeyed by the Service provider when processing the personal data, including such as Exclusivity of purpose (Section 7) and necessity requirements (Section 9). Thus, location data may be utilised only for the intended purpose and only to the extent necessary in the light of the intended purpose.

How may location data then be processed in practise? In provision of a typical location-based content service, be it for example a map service, there is no need to know the location of the user after the ordered location-specific content has been delivered. It is also hard to argue why the processing of location data would be necessary for other justifiable purposes. One question is, whether location data should or could be included in the bill.

The Tele Privacy Act provides that the identification data must be erased after the termination of a call. Certain information can be processed for determining telecommunications bills and interconnection payments. These exceptions do not concern location data, but it is evident that also location data must be erased when no longer needed.

5.10. Positioning Technology and the Finnish Criminal Code

The Finnish Criminal Code includes provisions on breach of Personal Data Act or breach of Tele Privacy Act. In addition to these norms, the Criminal Code does not include many norms that would control or limit utilisation or collection of location data or other utilisation of positioning technology.

The norms on violation of privacy and defamation, including provisions on illicit viewing, have been renewed in Finland. The amended provisions came into force on 1 October 2000. The new penal provision on illicit viewing (Criminal Code Chapter 24, Section 6) is as follows:

Joka oikeudettomasti teknisellä laitteella katselee tai kuvaa 1) kotirauhan suojaamassa paikassa taikka käymälässä, pukeutumistilassa tai muussa vastaavassa paikassa oleskelevaa henkilöä taikka 2) yleisöltä suljetussa 3 §:ssä tarkoitettussa rakennuksessa, huoneistossa tai aidatulla piha-alueella oleskelevaa henkilöä tämän yksityisyyttä loukaten, on tuomittava salakatselusta sakkoon tai vankeuteen enintään yhdeksi vuodeksi. Yritys on rangaistava.

As can be seen, only watching and recording is prohibited. The provision does not prohibit other technical surveillance. As an analogous interpretation is not allowed in the criminal law, the norm does not cover surveillance by using positioning technology. Prohibition of analogous interpretation seems to prevent application of other norms relating to protection of privacy in the criminal code.

It appears that there are no other norms in the Criminal Code, which might limit utilisation of positioning technology for surveillance. Thus, if utilisation technology can be used for surveillance of a person outside the scope of the Personal Data Act and the Tele Privacy Act, the Criminal Code does not prohibit the utilisation. This could be the case when, for example, an area is guarded by monitoring signals sent by mobile phones within the area. If the monitoring is not conducted by a teleoperator (thus leaving provisions of Tele Privacy Act on identification information unapplied) and if the person in question cannot be identified, the Personal Data Act and the Tele Privacy Act are not applied, and the surveillance appears to be legal in the light of Criminal Code. This question, however, needs to be analysed further before definitive conclusions can be made.

6. *Intellectual Property Rights Issues Related to Positioning Technology*

The rapid development of information technology has enabled effective delivery of digital content to the end-users. The concept “content service” refers to a variety of services where content, be it text, images, music, sound or other type of content is transmitted to the end-user, and the value-added is based on the delivered content.

In location-based content services the delivered content may be information on the location of the user, map, services and shops available in the neighbourhood, timetable information, etc. It is underlined that these services are ordinary content services where the delivered content is automatically customised with regard to the location of the user. In this respect most of the intellectual property rights (“IPR”) issues pertaining to the provision of location-based content services are not new and not unique to the location-based services. However, as the care-

ful observation of IPR-related questions is a key factor in successful provision of location-based content services, certain IPR-related issues are included in the scope of the project.

IPR-issues, especially those related to database protection, are analysed in more detail in a separate report in the project.

6.1. Content Production and IPR – Overview

Copyright

Copyright is the central form of legal protection of content production. Copyright protects literary and artistic works. All kinds of artistic works, texts, pictures, music, maps, databases etc. can be protected by copyright if the work is original enough for protection. Copyright can be characterised as a protection of *expression*, i.e. information or ideas as such is not protected by copyright, but the way this information or ideas are expressed can be protected.

Copyright consists of the exclusive right to dispose of the work by making copies of it and by making it available to the public. It can be generalised that all relevant utilisation of copyrighted material in the light of location-based services is within the scope of the exclusive rights of the rightholder, and the consent of the rightholder is always required for the utilisation of the material if the material is protected by copyright. Copyright subsists until the end of the seventieth year following that in which the author died.

In order to qualify for copyright protection the material must be original enough. Trivial material is not protected. It is possible that certain types of material used in relation to location-based services fall outside the scope of copyright protection. It should be remembered, however, that a collection of such material might form a database that in turn can be protected by copyright or the so-called *sui generis* protection (see below).

In Finland copyright always arises to the natural person who has created the protected work. The copyright may then be transferred in its entirety or in part for example to an employer.

Information Society Copyright Directive

The information society copyright directive (2001/29/EC) has not been implemented in Finland as of end of October. The government proposal for the changes to the Copyright Act has been given.

The anticipated changes to the copyright include, among other things, (i) clarification to the exclusive rights of the copyright holder, (ii) exemptions to the exclusive rights (such as temporary reproduction), and (iii) protection of technical measures protecting copyrighted works.

Generally the changes to copyright regulations bring a long-anticipated clarification to many complex copyright-related problems faced in the digital environment. Protection of technical measures could enable introduction of new products and services that have earlier been too sensitive to piracy. Certain express exemptions to the copyright also limit the liability risks of many intermediaries in the digital networks. The anticipated changes to the Finnish Copyright Act cannot be analysed in detail in here.

Database and Catalogue Protection

Database protection, also called *sui generis* protection, is a new form of protection based on EU directive 96/9/EC.

A database is defined as "...collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means." To qualify as a database, there must be (i) collection of material, (ii) the contents of the database must be capable of being individually accessed. This precondition renders mere collections of data without any instruments facilitating data retrieval outside the scope of protection.

The database is protected under the *sui generis* regime if there has been qualitatively and/or quantitatively a substantial investment in either obtaining, verification or presentation of the contents of the database.

According to the directive, the *sui generis* consists of a right to prevent extraction and/or re-utilisation of the whole or of a substantial part evaluated qualitatively and/or quantitatively, of the database. The right does not extend to the individual elements of the database.

The interpretation of the new database protection is cumbersome and it is difficult to forecast what are practical implications of the protection. It is probable that collectors and generators of different kinds of compilations of data, such as fixture lists, and other list relating to sports events will try to demand licenses for the utilisation of the data collected by them.

In practise most of the location-based content services are based on databases from which the location-specific content is automatically retrieved. Such databases will often be protected by the *sui generis* protection, and the databases may not be utilised without the consent of the rightholder.

The catalogue protection protects catalogue, table or program or any other production in which a large quantity of data are compiled. Such catalogue, table or program enjoys similar protection as databases under the *sui generis* right.

6.2. Spatial Data and IPR

Spatial data is usually a set of coordinates describing a location of a service, or a location of another item or fact.

It is evident that a single set of coordinates generated by the computer system or otherwise does not qualify for copyright protection. It is also probable that a single set of coordinates does not qualify for database protection: a single set of the co-ordinates as such does not form a database. Thus, a single set of spatial data as such is not protected by IPR at all and IPR does not set any limits for the utilisation of a single spatial data.

The situation is different when a collection of spatial data is examined. Such collection could be, for example, a collection of coordinates of all gas stations in Finland, a collection of coordinates of the best restaurants in Helsinki or a collection of coordinates good fishing spots in

Saimaa. As such collection is usually a collection of data arranged in a systematic way and individually accessible by electronic means, the collections can qualify for database protection. If obtaining, verification or presentation of the contents of the database has involved a substantial investment, the database is protected by the *sui generis* right.

Collections of spatial data can qualify for database protection giving the rightholder the exclusive right to utilise qualitatively and/or quantitatively substantial parts of the database. It should be remembered, that the database protection does not extend to the information contained in the database. Any third party has a right to collect the same information and form an identical database from the information collected.

In short, the databases produced by companies for the provision of location-based services are often protected as databases, which makes investments into the collection of such databases and offering of such services more viable. On the other hand, database protection complicates production of content services, as companies will have to ensure that they have the rights needed. Database protection may extend the protection in a surprising way.

In the directive 96/9/EC on the legal protection of databases it is stated in Article 7(5) that the repeated and systematic extraction and/or re-utilization of insubstantial parts of the contents of the database implying acts which conflict with a normal exploitation of that database or which unreasonably prejudice the legitimate interests of the maker of the database are not permitted.

Often a content service utilises only a single data of a database, but if the whole database is available for the service, the database has been made available to the public, which is the exclusive right of the rightholder. Also extraction of substantial part of the database is an exclusive right of the rightholder.

An example of database protection: A protected database includes spatial data of all companies in Finland. Spatial data of all Finnish gas stations would a very small part of the whole database, probably less than 1 percent of the whole database. However, as a database including spatial data of all Finnish gas stations could be valuable and collection of such information would require substantial investment, it is possible that spatial data of all gas stations of Finland would be deemed to be qualitatively substantial part of the whole database.

An real-life example of a catalogue protection (Copyright Council case 2000:5): a map containing information on good cloudberry areas within the Oulu region, in which 126 good cloudberry locations were marked, did not qualify for copyright protection. However, the information concerning the cloudberry locations in the map formed a protected catalogue. By publishing a part of the map containing 29 per cent of the catalogue, and most cloudberry locations in the Utajärvi region, a substantial part of the catalogue had been made available to the public and thus the rights of the rightholder had been infringed.

In practise the database right seems to limit effectively the possibilities of third parties to utilise a database without the authorisation of the rightholder and it is likely that the database protection will have substantial effect on the markets of location-based services.

6.3. Location Data and IPR

Generally the same rules apply with regard to IPR to location data specifying a location of a user as to spatial data: a single set of coordinates specifying a location of a user is not protected by copyright, but a collection of such coordinate information can form a database which is protected as a database or as a catalogue. Limitations for the use of a single location data derive from data protection regulation as described in Section 3.

It should be noted that the database protection or the catalogue protection belongs to the person or entity that has collected the database or catalogue. If the teleoperator is collecting a database consisting of location data specifying a location of a certain person, if nothing else has been agreed on, the database right to the database belongs to the teleoperator. The user and the teleoperator can agree that intellectual property rights to the database are transferred to the user.

Regardless of the IPR, data protection regulation gives the user a possibility to provide for the use of location data related to him. However, if location data is made anonymous, data protection regulation does not apply. It is possible that teleoperator collects anonymous location data pertaining to its users and utilises the data statistically for example in studying traffic flows.

It should also be pointed out that there exists no regulation which would oblige the teleoperator to hand over location data to the user or to any third party. Under the present telecommunications regulation it is up to the operator to decide under what terms and to whom it will provide location data. The Telecommunications Market Act includes certain obligations of operators in respect of services offered to the users, such as a right to obtain a subscription to a public telecommunications network (Section 15 item 1 of the Telecommunications Market Act), but no telecommunications market regulation includes any obligations that would oblige the teleoperator to offer location services. This right of teleoperators to choose whether and under what terms to offer location services may have significant consequences in respect of the market structure of the location-based services.

It remains to be analysed whether the general competition regulation would oblige teleoperators to offer location services under reasonable conditions.

6.4. Utilisation of Public Information Resources

In many location-based services publicly available information resources are important sources of content. There are various publicly available information resources in Finland that might come to question. Population Information System in Finland (Väestötietokeskus), land register and other property registers, National Land Survey of Finland (Maanmittauslaitos) and The Finnish National Road Administration (Tielaitos) are only examples of the various public information resources available.

Generally the law on publicity of public records (laki yleisten asiakirjojen julkisuudesta) regulates the availability of information in public resources. In many fields there are more detailed regulation on the availability of the information. For example, väestötietolaki includes regulation on how information in Population Information System may be utilised. The law includes provisions on how the register may be connected to other information system. The Law on Land Register includes regulation on how land register information is available.

Due to the variety of public information recourses and the horizontal nature of the regulation, the points of interest in the field of public information recourses should be identified. One possible generic research subject would be the applicability of IPR, especially database right, to the information retrieved from the public information resources.

7. *Liability Questions Pertaining to the Provision of Positioning Services and Location-based Services*

Utilisation of location data often involves navigation, transportation or traffic. It may also be used in emergency situations for different purposes. It is easy to foresee how a failure to provide a requested location data or location-based service, a mistake in provision of the service, or merely a low quality of the service may cause considerable damages. Thus the liability questions related to the provision of location-based services seem to be essential for Service Providers.

In this Section liability questions related to provision of location service and location-based services are analysed the point of view being in the legal liability to compensate damages incurred. The question of liability for damages is a very broad legal field, and here only some typical liability cases can be looked into.

Although criminal liability issues are left untouched, it is noted that a criminal offence is usually a ground for a damage liability and obligates the offender to compensate the damages caused by the crime (including damages of third parties).

7.1. Different grounds for Damage liability

The general law determining liability for damages in Finland is the Damages Act. However, the Damages Act is not applied in contractual relationships, for which general principles of Finnish contractual law are applied. In most cases commercial services utilising location data are based on an agreement between the user and the service provider, and are thus outside the scope of the Damages Act. The liability issues in contractual relationships are analysed in Section 7.2.

According to the Tort Liability Act (412/1974), who intentionally or in negligence causes damage, is liable to compensate for the damage caused. As a main rule only personal injury and property damages are compensated. However, also a economic loss is compensated where the injury or damage has been caused by an act punishable by law or in the exercise of public authority, or in other cases, where there are especially weighty reasons for the same.

Certainly there are innumerable cases where damage can be incurred in an activity where positioning technology is utilized, and all those cannot be analyzed here. But what are the typical cases where a damage under the Tort Liability Act could be caused in utilization of positioning technologies? The most relevant field of activity outside contractual relationships seem to be public services, where the availability or provision of the service is not depended on an agreement but on the nature of the service and on obligations of public authorities. The issues related to the liability of the state or other damages caused in exercise of public authority in analysed in Section 7.3.

7.2. Contractual Liability

At first look the liability questions in contractual relationships are pretty straightforward. Under the main rule, the parties are under the principle of freedom of contract free to agree on the terms of the contract, the choice of law, limitations of liability etc.

Starting point for contractual liability is, naturally, that the party in breach of a contract is to compensate for damages caused by the breach of contract. A contractual party is in breach of a contract if he has not fulfilled his contractual obligations. Thus, the decisive factor for assessing contractual liability is assessing the obligations of parties and whether the parties have fulfilled their obligations under the agreement.

It is naturally impossible to determine general rules for contractual liability in provision of location-based services. The liability depends on what has agreed to be the obligations of the parties. If the service provider has committed itself to always provide high-quality location data without delay at the request of the customer, the service provider is in breach of contract

if he has failed to do so and is thus liable for damages incurred. It can thus be concluded that it is essential to describe in detail the quality and limitations of the service when entering into an agreement on provision of a location-based service. If the limitations in the quality, usability and availability of the service have been described in sufficient detail in the service description of the service agreement and in the advertisements, the service provider can effectively control its contractual obligations and liability.

What damages need to be compensated? The contractual liability covers personal damages, property damages and also economic loss. The liability is limited by the foreseeability of the damage, and the causal relationship between the breach of contract and the liability: the damage must have been foreseeable to the party liable for the damages, and the damage must have been caused by the breach of the contract.

The parties are free to agree on the liability as they choose. It is thus generally possible to agree on limitations of liability of the service provider. It is in principle possible to disclaim any and all liability for the service and its errors or non-availability. Although freedom of contract is the general starting point, there are, however, several limitations to it. For example, the possibility to limit liability for damages caused intentionally or in gross negligence is limited.

It is generally accepted that surprising and unreasonable terms of a standard agreement (“vakiosopimus”) can be non-binding. This could be especially important in relation to location-based services, as it can be expected that very often the agreement on provision of a location-based service is a standard agreement. Thus, if the service agreement includes surprising or unreasonable limitations of liability, such limitations of liability could be non-binding. The agreement terms should reflect the impression and information given in the service descriptions and advertisements for the service. For example, if the consumer has, on the basis of advertisements, an expectation of a service providing at all times accurate and error-free navigation information, the service provider could have liability for shortcomings in the quality of the service in spite of limitations of liability in applicable agreement. On the other hand, if the customer is made aware of quality limitations of the service, the service provider could limit its liability more effectively.

The compulsory legislation provides also other limitations to the freedom of contract, the most important limitations relating to consumer legislation, which includes detailed compulsory protection to consumers. The consumer protection legislation includes, among other things, stricter standards to liability of merchants. A Service Provider cannot limit its liability towards a consumer more than allowed under the Finnish Consumer Protection Act. Liability and quality requirements are based on overall judgment. What is then the measurement rod in assessing the liability and quality requirements set for a location-based service under the Consumer Protection Act? Attention will probably be paid, among other things, to the general quality of similar service in the market, and to the marketing and other information concerning the service made available by the service provider. On the basis of this the reasonableness of the limitation of limitation and other contractual terms is assessed. The problem is, naturally, that often the marketing material does not include sufficient information on the quality and nature of the service. It is of highest importance for a Service Provider to communicate the nature, purpose, limitations and quality of a location-based service in order to avoid surprising liability claims.

There are no special provisions about the liability of location-based service provider.

It is impossible to go through the detailed and broad range of issues related to contractual liability in different cases. It can be shortly concluded that

- as a main rule freedom of contract prevails and the liability issues can be agreed on;
- a decisive factor in contractual liability are contractual obligations, and the service provider can in many cases effectively limit its contractual liability by limiting its contractual obligations;
- if general terms and conditions of the service provider are applied to the service (which usually is the case), the terms and conditions should not include unexpected and unreasonable terms, but should reflect general information and service description given about the service;
- the freedom of contract does not prevail in all cases. Especially in consumer relationships the freedom of contract is limited and the quality and liability requirements are more stringent.

7.3. Public Services

In provision of public services, the relationship between the authorities and the service user is not based on contract but directly on applicable regulations. The regulations applicable vary on the nature of the service, the general law being the Damages Act. However, several laws include special regulations concerning obligations of public authorities, and these obligations determine the limitations of the liability of the state.

There are several cases where a state or other public authorities could be the party utilizing positioning technology or providing public service with positioning technology. The state has assumed a liability for the maintenance of certain services, such as the maintenance of public roads and the maintenance of nautical chart. A failure to maintain public roads or a mistake in the nautical chart could lead to a liability for damages incurred. The following precedents of Supreme Court are examples of state's liability:

KKO 1996:71

Jalankulkija oli loukkaantunut kaatuessaan yleiseen tiehen kuuluvalla erillisellä hiekoittamattomalla jalankulku- ja pyörätiellä. Valtio tienpitäjänä katsottiin velvolliseksi pitämään tie jalankulkuliikennettä tyydyttävässä kunnossa hiekoittamalla se liukkauden torjumiseksi. Valtio velvoitettiin suorittamaan jalankulkijalle vahingonkorvausta.

KKO 1992:95

Vahingonkorvaus - Tienpitäjän vastuu

Jalankulkija oli liukastunut kävellessään taajaman keskustassa jalkakäytäviä vailla olevan yleisen tien lumista ja jäistä reunaa pitkin ja kaatuessaan loukkaantunut. Huomioon ottaen yleisistä teistä annetun lain 11 ja 12 §:n säännökset valtio tienpitäjänä ei ollut velvollinen hiekoittamaan jalankulkijoiden käyttämiä tien reunoja. Valtio ei siten ollut vastuussa jalankulkijalle aiheutuneista vahingoista. (Ään.)

KKO 1989:111

Merioikeus - Vahingonkorvaus - Julkisyhteisön korvausvastuu

Kauppa-alue oli ajanut karille, josta ei ollut tiedotettu, vaikka samalla vesialueella oli jo 10 vuotta aikaisemmin merenkulkuhallituksen merenmittauksissa todettu kari noin 9 metrin syvyydellä.

Kari sijaitsi vesialueella, jota merikortin ja viitoituksen mukaan ei ollut tarkoitettu merenkulkuun jutussa ei myöskään ollut esitetty näyttöä siitä, että aluetta mahdollisia satunnaisia poikkeuksia lukuunottamatta olisi käytetty merenkulkuun. Koska merenkulkuviranomaiset siten eivät olleet havaitun karin merkitsemisen tai siitä tiedottamisen suhteen tuottamuksesta laiminlyöneet vellli-

suuttaan, valtio ei ollut velvollinen korvaamaan karilleajosta aiheutunutta vahinkoa.

Kysymys myös jäänmurtajien antamien n.s. reittipisteiden merkityksestä.

The state has also been found liable for a failure to provide a traffic sign to warn traffickers about frost heave (“kelirikko”).

The presented cases can be summarized as follows: if the state has assumed a responsibility for a certain service, it has a liability for providing the service and for errors in the service (such as providing nautical charts). However, such responsibility must be expressly stated in the law.

Corresponding liability could arise in relation to provision of public service with the help of positioning technology. However, the criteria for liability depend entirely on the nature of the service and applicable regulation, and no general conclusions can be made.

8. Contractual Issues Related to Provision of Positioning Services and Location-based Services⁵

The contractual questions pertaining to position technology and services are very close to the questions of mobile e-commerce. It is very hard to identify any contractual questions, which has relevance only to the position technology and serviced based on it. The same applies also to the regulations. For this reason the questions analysed in this section are in a relatively general level.

The legal problems are different a contract covers only one service, which happens instantly, or if the same contract covers a longer period with numerous service-transactions. Therefore it is practical to separate the contracts to 1) Long-term contracts 2) Single-transaction contracts. The table 8(a) illustrates some of differences between these two groups.

⁵ This Section has been written by Ville Oksanen

Table 8(a): Classification of Contracts

	Long-term contracts (LTC)	Single-transaction contracts (STC)
The tool with which the contract is made	Varies	Mobile terminal
Value of transaction	Varies, can be high	Typically quite low
Identification of the User	Necessary	Normally not required
Timing of the contract	Normally before the provision of the service	At the moment the service is needed
Right to cancel the service	Yes	Not required
Information requirements	Relatively easy to fulfil	Difficult to fulfil

The most problematic questions can be found from the STCs. The main reason for this is that during the time the most of the current legislation was made, mobile e-commerce was not yet in the radar screens of the legislators. Therefore the regulations impose requirements, which are very hard or almost impossible to fulfil with current technology. Another reason for the problems is that the traditional legal theory does not provide adequate terminology, which would take account the technical development.

8.1. Contracting parties

The first question, which has to be answered, is which are the contracting parties - or more exactly with whom the customer makes the agreement. The answer varies naturally case by case, but the defining factors are identifiable.

In a typical case the customer sends SMS-message to a certain phone number and receives later another SMS-message with the required information from a server. The cost of the service is included to the customer's regular phone bill. At the moment the teleoperators produce most or all of the functions pertaining to the transactions. Even if the service is based on information, which is produced by an external source, the user does not typically receive any information.

The situation is most likely going to change in the future. The different functions will diverge to independent services. The reasons for this development are twofold. First of all, the competition regulations referred to earlier in this report.

Second trend, which affects the situation, is the transition to IP-based traffic. In the future, most of the mobile location-based services are bought straight from the Internet and the role of the teleoperator will decrease to the transferor of IP-traffic (and to give possibly the location of the hand-set). In this kind of environment, the natural contract partner will be the location service provider.

The general principle, which can be derived from this, is that the agreement is made with the company, which processes the order. The exception to this rule is the situation, in which the teleoperator (or some other third party) is hired to do the processing.

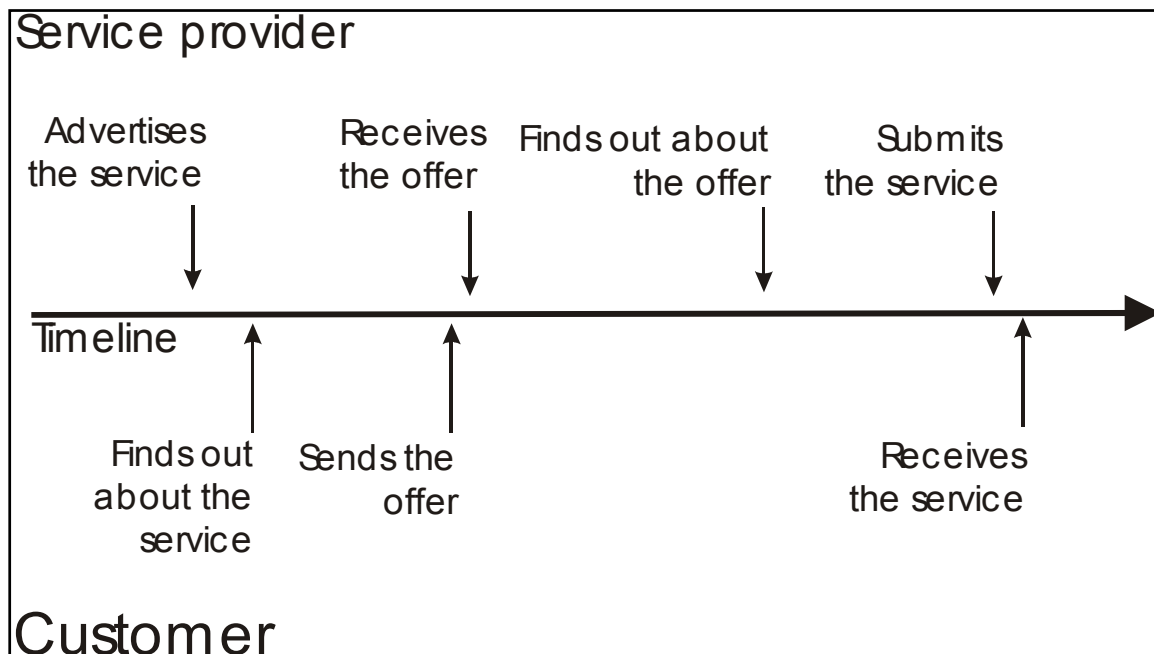
In the world of diversified services, the location service contract is often not enough alone. Each of the services, which are needed for the transaction, will most likely need a separate agreement between the user and service provider. The legal questions, which follow from this, are not anymore in the scope of this section.

8.2. Contract Formation

Generally speaking, there are no formal requirements under Finnish law for the formation of a contract. Contracts may be formed by oral or written agreement or by the conduct of the parties. However, some statutes and regulations impose specific writing or signature requirements for the contracts. Also, certain types of contracts can't be enforced in a court of law if they are not in specific written form (real estate contracts) or registered in the court (marriage contracts).

Electronic commerce presents new challenges to existing contract principles in several areas. Issues such as offer and acceptance, the location of the contract, and implied terms and conditions offer new scope for disputes between contracting parties. As yet, there is little or no case law in Finland with respect to electronic contracts and it is very hard to know how the courts

will resolve these issues. On the other hand the legislation is at the moment being updated. Forthcoming E-commerce act and E-signature act will clarify most of open questions.



In Finland, a contract is formed through the exchange between the parties to the contract of an offer and an acceptance of that offer. In electronic transactions, it may not always be clear which party is making an offer, in the contract sense, and which one is accepting. For example, an advertisement is traditionally not viewed as an offer to sell but as a willingness to consider offers to purchase. The prospective buyer makes the offer when he or she offers to buy the advertised goods or services. This may be done in person, for example in a retail store, or remotely, when a person fills in the order form in a web-catalogue.

The question is, if this model is outdated with respect to location-based services (and to all mobile e-commerce), because most of transactions are in reality based on information, which received from the advertisement. Is it logical to give such legal value to the last step? Even the new The E-commerce directive does not give any answer to this question and therefore it is up to the national legislation to decide when the contract is legally binding. The customer's and service provider's interests are naturally opposite in this question.

What it would mean then for the service provider, if the contract would be binding after the customer sends the order based on the marketing information? To begin with the service provider should have to be always able to provide the service, because otherwise the customer

could claim contract-based damages. Secondly the amount and the quality of information given in the advertisement should be much higher (a typical example is requirements caused by the privacy legislation). Therefore it is very obvious that this is a very problematic outcome for the service providers.

In Finland this question luckily is more or less academic, because the parties may agree in a contract, what is the exact moment when the contract becomes legally binding. Consequently the service agreements should always have an explicit clause, which states that the contract is not binding before the service provider accepts customer's order.

8.3. Cancelling the offer

The contract is completed when confirmation of acceptance is communicated to the offeror. Until that time, the offer may be withdrawn in some jurisdictions. In Finland the offer may only be withdrawn if the offeree has not find about the offer yet. In everyday face-to-face transactions (like in cash counter), acceptance is communicated instantly by receiving payment and handing over the goods. The time frame is also very narrow if the acceptance is fully automated, which will be most likely the case in most of location-based services.

The easiest solution for this question would be to make it technically impossible to withdraw the offer. In some cases this is possible, because the legislation requires that the customer have to have an opportunity to cancel the order.

8.4. Electronic Signature

When parties form agreements that they expect will be given legal effect, a signature may or may not be part of the process of contract formation. A signature is one type of evidence that that one of the parties intended to enter into a legally binding relationship, but it is not the only type. In most cases, a signature may not even be a necessary piece of evidence. Just what kinds of evidence of the intention of the parties to enter into a binding agreement will be used in any specific transaction will vary according to the context, including the subject matter for the particular transaction, the communications media the parties are using, the course

of dealings between the parties, and the normal business practices in the market or industry. In certain situations, the law may require a party seeking to enforce its rights to produce a writing signed by the party against whom enforcement is sought, but such requirements are scarcely universal.

In practise it is possible to create services without using any electronic signatures. So far there is very little (if none) examples of wide scale commercial use of digital signatures in any field of electronic commerce. The location-based service providers have to be able to identify the user reliably in case of LTC and also to the lesser degree in STC. The question is, does electronic signatures play some kind of role in the identification process. At least the mobile handset based solutions have so far relied on passwords or pin codes as method of user authorisation, and it has worked generally speaking quite well. Does the reduced legal liability overweigh the technological and financial burden the signature system imposes? The answer depends heavily on cost/benefit analyse. Another factor, which has to be taken account, is the likelihood that someone tries to exploit the system. As long as the value of single transaction stays low, this risk is diminutive.

The conclusion to the question about electronic signatures is that at the moment they are not essential for the location-based services. The user authentication can be handled reliably enough by using other methods. The typical uses of location-based services do not cover areas, in which are legal requirements for the form of the contract. This does not mean that electronic signatures will not have any role in future for location services. It is possible that in future there will be inexpensive and technologically easy enough solutions, which will also serve the needs of low-value transactions.

8.5. Choice of Law

In the absence of an agreement to the contrary, (generally speaking) the law of the jurisdiction where the contract is concluded (the location of the accepting party) will govern the contract. In an electronic commerce environment, where a seller may be dealing with potential buyers from around the world, it may be advantageous for the seller to try to control the jurisdiction of the contract. By selecting a favourable jurisdiction, the seller may be able to exclude or

limit implied warranties and to limit its liability in business to business-relations. The possibility to select the jurisdiction is limited in the consumer contracts.

The EU first addressed the choice of law problem in international consumer contracts with the 1980 Rome Convention on the Law Applicable to Contractual Obligations. Under Article 3 of the Rome Convention, the parties to a contract are free to select the governing law; however, Article 5 provides that a choice of law provision in a consumer contract may not deprive the consumer of the benefit of mandatory consumer protection laws in effect in the consumer's country of habitual residence. Such mandatory consumer protection laws include those prohibiting unfair contract terms, limiting the enforceability of standard form contracts, creating rights of cancellation during a "cooling off" period following the formation of the contract, or requiring that the seller make certain disclosures. These choices of law provisions have a dispute resolution counterpart in the 1968 Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, which governs questions of judicial jurisdiction among various European countries. Article 13 of the Brussels Convention provides that while a consumer has the option to bring suit against a business in either the consumer's or the business' home country, the business may only bring suit against the consumer in the consumer's country.

In July 1999, the Commission adopted a draft Regulation on Jurisdiction, Recognition and Enforcement of Judgments in Civil and Commercial Matters. After adopted by the Council of Ministers 22 December 2000, this regulation replaced and updated the 1968 Brussels Convention. The Article 16 defines the possible locations of the proceedings:

Article 16

- 1. A consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or in the courts for the place where the consumer is domiciled.*
- 2. Proceedings may be brought against a consumer by the other party to the contract only in the courts of the Member State in which the consumer is domiciled.*
- 3. This Article shall not affect the right to bring a counter-claim in the court in which, in accordance with this Section, the original claim is pending.*

It's consequently possible that any EU merchant who operates an electronic service that can be accessed by a consumer will be at risk of being haled into court in the country of the consumer's habitual residence in the event of litigation with the consumer. This would be true even if the merchant operating the electronic service had not taken any steps beyond informing about service on the Internet and had taken no more active steps to target consumers located outside the Member State where the merchant's business was established. This is a stricter standard than the one contained in Article 13 of the Brussels Convention, which provides that a merchant is subject to the jurisdiction of the courts of the consumer's country only if the conclusion of the contract was preceded by a specific invitation addressed to the consumer or by purchasing advertising targeted at the country of the consumer's habitual residence, and the consumer took the steps necessary to conclude the contract from within the consumer's own country.

Consequently if a service provider wants to limit the geographical dimension of its legal risks, a technical solution is needed to block the consumers from unwanted countries. In traditional phone-network this is relatively easy task but the situation will be much more complicated after the traffic is mostly IP-based.

8.6. Other aspects of consumer protection

In 1997, the EU adopted a directive on the protection of consumers in respect to distance contracts (the Distance Selling Directive). The Distance Selling Directive is supposed to promote online commerce by providing consumers with a guarantee that they will be protected by their own national consumer protection regime when they enter into distance selling contracts. Distance selling is defined as the conclusion of a contract regarding goods or services whereby the contract between the consumer and the merchant takes place by means of technology for communication at a distance. Consumers felt the need for special protections in this area because of the risks of invasions to individual privacy by aggressive marketing techniques, inadequate or improper information being provided to the consumer by the merchant, and risks of fraud or error in card payment services used to make payments under distance selling contracts. In addition, the rights granted to consumers through the enactment of the Distance Selling Directive's provisions into national law might not be waived by the consumer.

The Distance Selling requires that a transaction be completed within thirty days or notice must be sent to the consumer of the situation giving the consumer the option to cancel the transaction. The Distance Selling Directive covers most forms of direct marketing, including catalogue mail order, telephone sales, direct response television sales, newspapers, magazines, and e-commerce. The Distance Selling Directive requires that a consumer must be given certain minimum information, both at the time of contract solicitation and at or before the time of delivery. Written confirmation of information must be received by the consumer in some form of "durable medium" accessible to the consumer. Consumers must, subject to certain exceptions, also be given a "cooling-off" period of at least seven working days. Where the consumer exercises his or her right of withdrawal from the contract, the supplier is obliged to reimburse the consumer for any sums paid.

In an effort to protect merchants from unreasonable burdens in consumer transactions, certain types of transactions are exempted from the coverage of certain Distance Selling Directive protections. For example, unless the parties have otherwise agreed, the consumer's seven-day right of withdrawal does not apply to contracts

1. For the provision of services if performance has begun before the seven days are up;
2. For the supply of goods or services the price of which is dependent on fluctuations in the financial market which cannot be controlled by the supplier;
3. For the supply of goods made to the consumer's specifications or clearly personalized, or which are likely to deteriorate or expire rapidly;
4. For audio or video recordings or computer software, which were unsealed by the consumer;
5. For the supply of newspapers, periodicals, or magazines; or for gaming or lottery services.

This means that STCs fall out of the scope of the directive based on section 1. or 3. At the same time it is possible that the directive fully applies to LTCs.

The most difficult part of Distant Selling Directive is the requirements for information, which has to be supplied to the consumer before and after the transaction. The required amount of information is too high to be transmitted to mobile phones especially with SMS-messages. Even with WAP it is still very unpractical because most of the phones do not have decent sized screens yet. Therefore it would make more sense to store the information somewhere

else, in practise to the WWW. The problem with this is that the Distant Selling Directive and the Finnish Consumer Protection Act do not recognize this kind of conduct. Another practical problem is that at present the service providers cannot expect that everyone have an access to Internet. The situation will be clearer after the Finnish consumer protection agency will give its instruction about E-commerce.

9. Utilisation Of Positioning Technology In Certain Fields

9.1. Provision of Information Society Services

Background

The directive on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (2000/31/EC, hereinafter ecommerce directive) sets fort general principles for the provisioning of information society services. The purpose of the directive is to harmonise certain important aspects of provision of services over the publicly available data networks. The definition of “information society service” is somewhat complex. Suffice to say here that it generally covers all services provided over the information networks.

Generally taxation issues and lottery regulations are exempt from the breach of the directive.

Country of origin –principle

The directive was implemented in Finland in year 2002 with the law “Laki tietoyhteiskunnan palveluiden tarjoamisesta, 458/2002) and came into force 1 July 2002 (the law hereinafter referred to as the “ecommerce Act”). In principle the most important aspect of the ecommerce Act is the principle of country of origin: Within EU the country of origin –principle is applied to information society services, meaning that the laws of the country where the service provider is established are applied to the provision of the service. This means that other member states may not prohibit the provision of the service, and the service provider does not have to

comply with the regulations of all member states, but merely with the regulations of the member state where the service provider is established.

There are several exceptions to the country of origin principle, most important of which are the following: intellectual property rights, contractual obligations in consumer relations, and unsolicited commercial communications.

The benefits of the country of origin –principle can be substantial in many heavily regulated fields. The exceptions should be remembered when implementing location-based services. For example, for contractual obligations concerning consumer contracts the country of origin -principle does not apply.

General Information to be Provided and Information Related to Commercial Communications

The ecommerce Act includes several detailed obligations for a service provider to provide information concerning the service and concerning the service provider. Under the general obligation to provide information the following information must be provided by the service provider (the list taken directly from the directive, the provisions in the Finnish ecommerce Act are identical):

- (a) the name of the service provider;
- (b) the geographic address at which the service provider is established;
- (c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner;
- (d) where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register;
- (e) where the activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority;
- (f) as concerns the regulated professions:
 - any professional body or similar institution with which the service provider is registered,
 - the professional title and the Member State where it has been granted
 - a reference to the applicable professional rules in the Member State of establishment and the means to access them

Furthermore, under the general information obligations the service provider must, when referring to prices, give pricing information clearly and unambiguously.

In addition to the general information obligations, there are detailed provisions in the e-commerce Directive concerning commercial communications, which are part of, or constitute an information society service. The following detailed requirements are set forth in the Directive:

- (a) the commercial communication shall be clearly identifiable as such;
- (b) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable;
- (c) promotional offers, such as discounts, premiums and gifts, and bodies where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously;
- (d) promotional competitions or games, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions for participation shall be easily accessible and be presented clearly and unambiguously.

The implementation of these obligations into Finnish law included changes also to the Consumer Protection Act and to the Act on Unfair Business Practises, where corresponding obligations were enacted.

Contracts Concluded by Electronic Means

The e-commerce directive includes also detailed provisions concerning conclusion of contracts by electronic means. The purpose of the directive is to facilitate utilisation of electronic communications for concluding contracts.

The directive includes also information and procedural obligations concerning conclusion of a contract. Such obligations include, among other things, an obligation to make available contractual terms so that the recipient can save or copy them.

Because the treatment of contracts is a horizontal issue and not specific to location technology, we cannot analyse details of the contractual obligations and norms in the e-commerce Act in this context.

Liability of Certain Providers of Information Society Services

The ecommerce Act includes detailed safe harbour regulations for certain intermediary service providers. Under Section 4 of the directive providers a mere transmission, caching or hosting shall not be liable for the information transmitted, cached or hosted, if the detailed conditions set forth in the directive are fulfilled.

These safe harbour principles are welcomed clarification for the situation for teleoperators. Especially liability of a provider of a hosting service has been unclear. Now it has been established that storage of information as such cannot establish liability for the stored information.

The ecommerce directive states as follows:

Where an information society service is provided that consists of the storage of information provided by a recipient, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

- (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
- (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

If a location-based service includes a service under which user can publish or store their own messages or information (for example, location-based messages for any other users), the service provider is not liable for the information unless (i) service provider is aware of the information, (ii) it does not act expeditiously to remove or to disable access to the information after obtaining knowledge of the illegality of the information, or (iii) the publisher of the information is acting under the authority of the Service Provider (for example employee fulfilling his employment obligations). The problem, of course, is to determine at what constitutes sufficient knowledge.

Fortunately the Finnish implementation of the directive clarifies the situation: it is provided in the Finnish ecommerce Act that the service provider need not act prior to receiving a court order regarding the illegal activity. The parties who feel their rights violated need thus to obtain a court order. There are certain exceptions to this, most important being special “notice

and take-down” procedure established for preventing infringements copyright and related rights. The details of the procedure cannot be described here. Suffice to say that under the procedure copyright holders can directly contact the service provider and order the access to the infringing material to be removed.

As a generalisation about the situation in Finland it can be concluded that if a service provider is not deemed to be the publisher of the information, he cannot be made liable for the information published if he acts in accordance with the court orders or notices from copyright holders. This eases establishment of new services enabling publishing and storing of users’ own content.

It should be observed that the ecommerce act nor the directive does not specify under what conditions service providers would be liable for the information, but merely state conditions under which service providers are never liable for the information.

9.2. New Act Concerning Freedom of Speech

The Government proposal for a new Act on Freedom of Speech (Sananvapaus laki or Laki Sananvapauden käyttämisestä) is currently in the Finnish Parliament. The Act would clarify the current, to some extent obsolete, legislation concerning public information. The Act would replace the separate Acts concerning different fields of mass communication.

The proposed Act includes some difficult provisions. For example, some of the provisions would mean that, for example, a provider of a chat-service could be made liable for the contents and information published by the users of the chat service. It would also prescribe an obligation to collect and save identification information of all persons publishing content through the chat service. Should these provision be passed into a law, many chat-services in Finland would probably be shut down because the service providers would not be willing to risk the liability for the contents. Furthermore, collecting of the identification information would be extremely difficult.

The Act should be observed by all Service Providers enabling users to publish in one way or another their own content. It is uncertain when (or at all), and in which form, the Act will be enacted.

9.3. Protection Of Privacy In Employment Relations

On 1 October 2001 the Act on Protection of Privacy in Employment Relations entered into force in Finland. The Act is a result of long legislative work. In the late 90's a governmental proposal on the same issue was dismissed by the Parliament and sent back to the ministry for preparation.

The Act sets forth the framework under which employer is allowed to utilise personal information of the employees. As a main rule Section 3 § of the Act provides that employer may process only such personal data that is directly relevant with respect to the employment relationship. This provision is compulsory and cannot be bypassed with the consent of the employee.

Another important provision from the point of view of positioning is Section 9 § on procedures for organising technical surveillance. According to the said Section technical surveillance must be handled under the co-operation procedures (yhteistoimintamenettely) set forth in the Labour law of Finland.

Finally, the employees must always be informed about the surveillance used by the employer.

The Act as such does not give the employer new rights to monitor or collect information, but monitoring and information processing must always be based on other legal grounds. Furthermore, the Act does not prevent monitoring or surveillance without the consent of the employee. The Act merely sets forth procedural requirements and the compulsory prohibition for collection information not directly relevant with respect of the employment relationship.

In short, the Act has brought a welcomed clarification to the relationship of an employer and employee. Surveillance is allowed if it is directly relevant with respect to the employment

relationship. Thus, the question boils down to the following: when would monitoring of an employer be directly relevant with respect to the employment relationship?

Often utilisation of different kinds of fleet management systems can be deemed directly relevant. For example, a truck or a taxi company probably has a justifiable need to be able to control its fleet.

In case of an employer purchasing a fleet-management system from a service provider, the legal grounds for the utilisation of the fleet management system is based on the employer's right to process personal data. The Service provider of the fleet management system is acting merely under an assignment from the employer, and does not need to have other ground for the processing of personal data. (Personal Data Act, 8.1, item (7)). If the employer is entitled to process the data, the service provider is also entitled to process such data to the extent the processing is limited to that necessary for carrying out the assignment. The New Tele Privacy Directive might, however, impose certain obligations also to the Service Provider, as has been described in Section 4.

9.4. Positioning Of Persons under Guardianship and Elderly People

Generally the question about positioning of persons under guardianship can be divided into two main threads: (i) positioning of minors by the parents and (ii) positioning of an person that has been set under guardianship by a court.

The benefits of positioning minors and persons under guardianship in certain cases are clear. Positioning enables, for example, parents to more effectively monitor the activities of the children, adding security. Naturally the side effects of such monitoring are evident: the violation of privacy of the minor.

Generally under the Finnish regulations the parents have a right to decide over matter of the children under their custody (in Finnish "huoltaja", which must be separated from "holhous"). This in theory applies also to personal matters. However, the principle of privacy of the telecommunications of applies even in the relation between a child and a parent. In such a relation

the privacy can prove to be very strong. For example, it has been questioned whether a parent can ever have a right to acquire a full list of phone calls made from a phone for which a child is the registered user (irrespective of the consent of the child).

The existing regulations only provide for the general principles applicable to the privacy protection of minors and to the rights and obligations of parents. Thus, the detailed interpretations of such regulations must be determined on case-by-case basis.

From the point of view of a Service Provider the questions are as follows: (i) when can a Service Provider allow a parent to consent on behalf of a child for positioning, and (ii) is a consent of a child sufficient for positioning by a parent, or do children enjoy compulsory protection against positioning by their parents. Unfortunately these questions must be answered on case-by-case basis.

9.5. Positioning Technology in Direct Marketing

The Section 21 of the Data Privacy Act states as follows:

Telecommunications may not be used for direct marketing without the prior consent of the subscriber if the calls to the called subscriber are made by means of automated calling systems [...].

This out-dated provision in practise prohibits provision of non-ordered direct marketing to the user's mobile terminal, including marketing utilising location data.

In spite of the provision direct marketing is possible with the user's consent. The nature of the consent has not been specified. Therefore it is possible that the user gives any kind of consent to receive direct marketing. Consent could be given, for example, to a Service provider offering marketing on the basis of the location of the user.

The data ombudsman has pointed out that consents given for direct marketing should be easy to cancel, and the user should have a right to cancel its consent at any time.

The situation regarding direct marketing differs from country to country.

The new Tele Privacy Directive provides for a certain framework regarding direct marketing.

Article 13 of the directive states as follows:

1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.
2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.
3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.
4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.
5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

In short, direct marketing for natural persons is under the opt-in –principle, according to which subscriber’s consent must be obtained for direct marketing. The Paragraph 2 of the Article allows direct marketing with respect of existing customers for similar products or services that the customer has already purchased.

Opt-out –principle is applied to legal persons. Thus direct marketing can be directed to legal persons, but they have a right to prohibit direct marketing.

The existing regulations in Finland are mainly in line with the new directive, with a possible exception of paragraph 2 of Article 13. However, even the existing regulations can be interpreted so as to allow limited direct marketing within a customer relationship for products or services relevant for the customer relationship. At the very least information directly relevant for the existing customer relationship can be sent.

It should be borne in mind the abovementioned regulations on direct marketing concern direct marketing in general, and utilisation of location data in direct marketing will always require a prior consent of the data subject. A mere customer relationship under which location data can be processed by a Service Provider cannot usually suffice as a consent for utilising location data in direct marketing. Thus, the consent of the subscriber and/or the user should be obtained prior to utilising location data for direct marketing even in cases where the location data is available for the Service Provider.

Also the earlier presented e-commerce directive of the European Union includes provisions on unsolicited commercial communication. The Article 7 as follows:

1. In addition to other requirements established by Community law, Member States which permit unsolicited commercial communication by electronic mail shall ensure that such commercial communication by a service provider established in their territory shall be identifiable clearly and unambiguously as such as soon as it is received by the recipient.
2. Without prejudice to Directive 97/7/EC and Directive 97/66/EC, Member States shall take measures to ensure that service providers undertaking unsolicited commercial communications by electronic mail consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.

When the directive was implemented, the article 7 was taken into account by adding an obligation on the identifiability of unsolicited commercial communications to the Teleprivacy Act.

