

Location-based Services and General Privacy and Data Protection Principles

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



Report of the NAVI Regulatory Framework -project

**Location-based Services and
General Privacy and Data Protection
Principles**

Samuli Simojoki

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	2
1.1. <i>Navi-Regulatory Framework –project</i>	2
1.2. <i>What is Positioning Technology and How is it Utilised?.....</i>	4
1.3. <i>Positioning Technology from the Point of view of Fundamental Privacy Principles</i>	5
1.4. <i>Classifications and Concepts</i>	6
2. Fundamental Privacy and Data Protection Principles	6
2.1. <i>Defining Privacy and Data Protection.....</i>	6
2.2. <i>Privacy as a Personal Freedom in International Conventions.....</i>	7
2.3. <i>International Data Protection Regulations.....</i>	10
2.4. <i>Seeking General Data Protection Principles</i>	11
2.5. <i>Right for Information Self-determination?.....</i>	12
2.6. <i>General Data Protection Principles and Location-based Services</i>	15
3. Location-based Services in the Light of general Data Protection Principles.....	16
3.1. <i>Understanding Location Data and Positioning Technology.....</i>	16
3.2. <i>The Role of a Teleoperator as a Trusted Party.....</i>	17
3.3. <i>Actors in the Provision of Location-based Services.....</i>	19
3.4. <i>Security Obligations.....</i>	20
3.5. <i>Consent and Informing in the Context of Location-based Services</i>	21
3.6. <i>Obligations Related to the Provision of Information.....</i>	22
3.7. <i>Controller and Processor and the processing of Location Data</i>	24
4. Conclusions	26

Yhteenveto

[TO BE UPDATED]

Executive Summary

[TO BE UPDATED]

Location-based Services and General Privacy and Data Protection Principles

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

1. Background of the Report

1.1. Navi-Regulatory Framework –project

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.

This is the report under item (iii), analysing regulations under the general data protection principles.

It is underlined that this 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.

1.2. 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.

1.3. Positioning Technology from the Point of view of Fundamental Privacy Principles

Although the actual data protection regimes did not emerge prior to the 1970s, the question of data protection has been important earlier: data protection can be seen as one of the corner stones of broader privacy principles, basis of which can be traced back, at least, to the United Nation's Universal Declaration of Human Rights adopted on 10 December 1948.

While several countries have strong traditional approaches to privacy issues, certain converging principles and ideas are found behind most privacy regimes. Especially within Europe the privacy regulations have converged substantially in the recent years especially due to the activities of the Council of Europe.

In the earlier reports of the project it has been observed that the existing general data protection legislation does not always provided satisfactory guidelines for the development of positioning technology and location-based services. The new Directive on privacy and electronic communications (2002/56/EC) (New Tele Privacy Directive) will to some extent clarify the situation. However, it has been observed that a short analysis of the positioning technology and location-based services from the point of view of the general privacy and data protection principles could be in place.

In this report privacy questions related to the utilisation of positioning technology and provision of location-based services are briefly analysed from the point of view of general privacy and data protection principles. The report does not intend to be a thorough analysis of such principles or their applicability to positioning technology. The goal of the report is merely to show some alternative views how the privacy questions related to the subject-matter could be

approached. One goal is also to show how some of the basic concepts of data protection do not seem to fully cover the domain of the new location-based services.

It should be noted that there are several other issues related to personal freedoms and privacy issues that are relevant in processing of location data, which are not covered here. Such issues could be, for example, use of location data for surveillance by law-enforcement authorities and in case of emergency, relation of processing of location data to freedom of movement.

1.4. Classifications and Concepts

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

2. *Fundamental Privacy and Data Protection Principles*

2.1. Defining Privacy and Data Protection

There are no generally accepted definitions for privacy and data protection. Other report privacy is understood as a substantially broader concept than that of data protection, the latter covering strictly the issues related to the processing of personal data stored in databases. However, the definition of both concepts is somewhat complex. There are several ways to define privacy. One influential definition is given by Alan Westin states as follows:

“Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”.¹

This kind of a definition embodies many of the basic principles of data protection regulations, particularly those rules that enable persons to participate in and influence the processing of information about them. Furthermore, as Lee Bygrave has pointed out, a control-based defini-

¹ Alan F Westin: Privacy and Freedom (1970), Bodley Head

tion of privacy arguably lends the concept of privacy considerable normative force, as it allows privacy advocates to tap into the dynamic ethical undercurrent associated with the ideal of *self-determination*. In the Current Regulatory Framework –report of the NAVI Regulatory Framework project, the right of self-determination was identified as one of the central concept when analysing data protection and location-based services. However, it should be observed that data protection laws do not usually give persons an absolute right to determine how data concerning them is processed, but guarantee such right only under certain circumstances. In addition to the right of self-determination, another and, in the context of location-based services, even more important aspect of privacy could be referred to as the right to be informed.

Another way to define privacy has stemmed mainly from the US law practise and characterises privacy in terms of non-interference. This has been often referred to as a “right to be let alone”.

2.2. Privacy as a Personal Freedom in International Conventions

It can be generalised that the mainstream theoretical perspective on privacy has derived from the human rights tradition. There are alternatives to this approach. For example, Pamela Samuelson and some other US scholars have introduced a point of view of intellectual property rights to privacy. Also a market approach, based on economic theory, has been applied.

Governmental constitutions of different countries have for long acknowledged citizen’s right to certain personal freedoms. The US constitution is a classic example of this. Privacy has often been among such personal freedoms that have been protected, although its importance has been grown only after the Second World War. For example, the U.S. Constitution does not explicitly use the word "privacy" when discussing personal freedoms, but several of its provisions have been interpreted so as to protect its different aspects, the landmark cases being rather recent. The strongest protections in the US Constitution arise from the Fourth Amendment, which safeguards individuals in their persons, homes and papers from unreasonable searches and seizures.

There are several international conventions that cover issues related to personal freedom, most important of which are perhaps the following:

- Universal Declaration of Human Rights (1948)
- European Convention for the Protection of Human Rights and Fundamental Freedoms (1950)
- The International Covenant on Civil and Political Rights (1966)

The need for the Universal Declaration of Human Rights stemmed mainly from the atrocities of the Second World War. The preambles of the declaration state clearly this background and the goals of the declaration of human rights:

Whereas disregard and contempt for human rights have resulted in barbarous acts which have outraged the conscience of mankind, and the advent of a world in which human beings shall enjoy freedom of speech and belief and freedom from fear and want has been proclaimed as the highest aspiration of the common people,

Whereas it is essential, if man is not to be compelled to have recourse, as a last resort, to rebellion against tyranny and oppression, that human rights should be protected by the rule of law.

The European Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter “EHCR”) originates from the same ideas than the Universal Declaration of Human Rights, the preambles stating:

Considering the Universal Declaration of Human Rights proclaimed by the General Assembly of the United Nations on 10th December 1948;

Reaffirming their profound belief in those fundamental freedoms which are the foundation of justice and peace in the world and are best maintained on the one hand by an effective political democracy and on the other by a common understanding and observance of the human rights upon which they depend;

Being resolved, as the governments of European countries which are like-minded and have a common heritage of political traditions, ideals, freedom and the rule of law, to take the first steps for the collective enforcement of certain of the rights stated in the Universal Declaration.

The EHCR developed a pan-European framework for the interpretation of human rights principles through European Commission of Human Rights (set up in 1954) and the European Court of Human Rights (set up in 1959).

The article 8 of the EHCR is the most important with respect to privacy:

Article 8 – Right to respect for private and family life¹

Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The Art 17 of the International Covenant on Civil and Political Rights (ICCPR) of United Nations sets forth as follows:

“1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks”.

The declaration of human rights has not in its own right been often analysed from the point of view of privacy. This could be due to the fact that other international conventions, such as both the EHCR and ICCPR can be regarded as a more detailed implementation of the principles of the Declaration of Human Rights. Indeed, both EHCR and ICCPR have been widely interpreted and analysed from the point of view of privacy.

Case law developed around Art 17 of the ICCPR provides the clearest indication that the right to privacy in international law harbours core data protection principles. This is not necessarily the case with the EHCR: although the case law pursuant to Art 8 of the ECHR which touches upon data protection issues is relatively extensive, the case law of the European of Court of Human Rights regarding privacy has been mainly concerned with issues such as governmental surveillance, sexual rights, etc. The privacy of an individual with regard to data processing

activities of private entities has not been often touched by ECHR. However, the court has held that article 8 “may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals themselves”. However, the issue of whether or not Art 8 provides protection against the data-processing activities of private bodies has not been conclusively determined.

The focus of this report is the processing of location data, privacy and data protection. To be more precise, we are mainly interested in processing of location data by private entities such as providers of location-based services, employers, parents, guardians, etc. However, ECHR provides only very limited case-law regarding relationships of private individuals. Thus it appears that the above-mentioned international conventions provide only indirect guidelines for interpreting privacy related questions related to the location-based technologies with regard to private entities.

2.3. International Data Protection Regulations

As noted above, general idea about privacy as a personal freedom can be traced back rather far into the legal history. In spite of that, the emergence of data protection laws is, after all, recent. In most countries the first pieces of express legislation on data protection were not enacted before the 1970s. Already during those times the development of information technology was the driving force behind the data protection legislation. The principles of the existing general data protection regulations, including EU’s data protection directive, originate from those times.

Various legal instruments on data protection have been introduced in the international level. The most important of these instruments are the following:

- The Council of Europe Convention for the protection of Individuals with regard to Automatic Processing of Personal Data, 28.1.1981 (the CoE Convention)
- Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC, the Data Protection Directive)

- OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines)
- UN Guidelines Concerning Computerized Personal Data Files (UN Guidelines)

Among these instruments, the CoE Convention is probably the most influential. By December 2002 it has been ratified by 27 countries. The Convention is also the primary reference for the Data Protection Directive. Indeed, the recital 11 of the Directive states as follows:

“Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, *give substance to and amplify those contained* in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data”.

The OECD Guidelines and UN Guidelines are not legal binding on the member states of OECD and UN. They are “merely” guidelines created in order to encourage states to implement data protection schemes. At the very least, by signifying the international understanding of the importance of data protection questions, the guidelines have been instrumental in yielding data protection issues higher status.

2.4. Seeking General Data Protection Principles

Despite some differences, it can be generally concluded that the aforementioned international instruments are broadly similar on many points and main principles. The level of detail varies considerably from the rather general level of the CoE Convention into the detailed provisions of the Data Protection Directive.²

It can be concluded on the basis of the review of the International Data Protection Regulations, that there are certain general data protection principles to which the national data protection regulations are based upon, such principles focusing on the processing, collection, registration, storage, use and dissemination of personal data. However, it is not easy to extract

² See for example “Data Protection Law – approaching its rationale, logic and limits” by Lee A. Bygrave. Kluwer Law International, 2002, p. 30-56.

these principles from the international regulations. Bygrave has summarised basic data protection principles as follows:

- Personal data should be gathered by fair and lawful means (“fair collection principle”);
- The amount of personal data gathered should be limited to what is necessary to achieve the purpose(s) of gathering the data (“necessity principle”);
- Personal data should be gathered for specified and lawful purposes and not processed in ways that are incompatible with those purposes (“exclusivity of purpose principle”);
- Use of personal data for purposes other than those specified should occur only with the consent of the data subject or with legal authority (“use limitation principle”);
- Personal data should be accurate, complete and relevant in relation to the purposes for which they are processed (“data quality principle”);
- Security measures should be implemented to protect personal data from unintended or unauthorised disclosure, destruction or modification (“security principle”);
- Data subjects should be informed of, and given access to, data on them held by others, and be able to rectify these data if inaccurate or misleading (“individual participation principle”,); and
- Parties responsible for processing data on other persons should be accountable for complying with the above principles (hereinafter termed “accountability principle”).³

For the interests of this report especially the principles of necessity, exclusivity of purpose, security and individual participation are of high importance. These principles will be examined in more detail later in the report.

2.5. Right for Information Self-determination?

It is interesting to observe that a principle of self-determination is missing from the Bygrave’s list of general data protection principles. In fact, the general data protection principles do not include general, over-riding principle of self-determination: a data subject may not prohibit processing of his/her personal data if there are otherwise legitimate reasons for the processing of such data. For example, a debtor may not prohibit the creditor (for example a bank) from processing of personal data needed for the management of their contractual relationship.

³ Lee A. Bygrave: "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties", International Journal of Law and Information Technology, 1998, vol. 6, pp. 247-284.

In the end, even the CoE Convention and the Data Protection Directive do not recognise a general principle of self-determination. On the contrary, CoE Convention does not specify consent of the data subject as grounds for the processing of personal data. Similarly there are only certain cases in the Data Protection Directive where the data subject has a general right to prohibit the processing of personal data or where data subject's explicit consent is required for the processing of such data. These cases are exceptions to the main rule. Indeed, the recital 25 of the directive, summing the rights of a data subject, states that a data subject has a right "...even to object to processing in *certain circumstances*". Such circumstances are, for example, processing of personal data for direct marketing and processing of sensitive data (with several exceptions).

It should be observed that in spite of the lack of general informational self-determination, naturally a person has actually a wide range of control over the processing of his personal data by private entities: by choosing contractual partners and service providers a person can to some extent control which private entities are processing his/her personal data. A general informational self-determination, would, indeed, be impossible to implement.

However, there are various other sources where the informational self-determination has been deemed to be one of the very corner stones of the European data protection regime. For example, a former president of the European Court of Human Rights, Rolv Ryssdal, has explicitly stated, that the interpretation of the article 8 of the ECHR is developing towards a right of informational self-determination.⁴ The question remains, however, what could be the contents of such right of informational self-determination.

Let us try to find traces of informational self-determination from the existing data protection regimes. Legal manifestation of informational self-determination is clearly present in such provision of data protection laws which prohibit the processing of personal data without the consent of the data subject, or which give a data subject a right to object the processing.

⁴ R Ryssdal, "Data Protection and the European Convention on Human Rights", in *Data Protection, Human Rights and Democratic Values* (Strasbourg: Council of Europe, 1992).

The right of informational self-determination (understood as a prohibition right to process personal data without the consent of the data subject or data subject's right to object to such processing) is as such not very relevant in the context of processing of personal data for otherwise legitimate purposes. For example, in case of a customer relationship, processing of personal data is based not on data subject consent but, in the context of the Data Protection Directive, on the performance of a contract to which the data subject is party. In case a data subject has entered into a contract, personal data necessary for the performance of the contract may be processed. In such cases the rights of the data subject are protected, among other rights, by the data subject's right to be informed of the processing of personal data and by the data controller's obligation to process only data necessary for the pre-defined purpose. These principles and other principles mentioned in Section 2.4 that can with good grounds be seen as separate from the informational self-determination principle, do protect the same interests as the informational self-determination principle is supposed to cover.

In this report we are mainly interested in processing of location data by private entities such as providers of location-based services, employers, parents, guardians, etc, and not processing of location data by authorities for law-enforcement or emergency. It appears that within the context of location-based services, only rarely does processing of personal data take place outside of a contractual relationship of some kind, be it between the data subject and a Teleoperator, or between the data subject and a provider of a location-based service (Service Provider).

Thus, *in the context of the Data Protection Directive*, only rarely would a consent of a data subject be the sole grounds for the processing of location data, but the grounds for processing of location data would arise originally from a service agreement or other corresponding agreement between the positioned person and the Service Provider.

However, the recent Directive on privacy and electronic communications (2002/58/EC), The New Tele Privacy Directive, brings the principle of informational self-determination again to the foreground when discussing location-based services. As noted above, the Data Protection Directive does provide for informational self-determination in certain cases, although such right is not the main rule. The New Tele Privacy Directive adds to the category of informational self-determination the processing of traffic data and other location data relating to a

person. The Directive states clearly that traffic data and other location data may be processed only with the explicit consent of the user of the terminal.⁵ The consent must fulfil the stringent requirements for the consent set forth in the Data Protection Directive. The user of the terminal has a right at any time to withdraw his/her consent temporarily or permanently or otherwise generally prohibit the processing of location data. This right can not be bypassed contractually.

Thus, it can be concluded that the principle of informational self-determination, finding its embodiment in the recent directive, is an important right of the terminal user in the context of location-based services.

It should be noted that the New Tele Privacy Directive covers only providers of telecommunication services and providers of value added services, and the right of informational self-determination with respect to traffic data and location data does not directly apply with respect to other parties.

2.6. General Data Protection Principles and Location-based Services

As mentioned above, in this report we are especially interested of the principles of necessity, exclusivity of purpose, security and individual participation. Within the context of location-based services and processing of location data these principles could be reformulated as follows:

- Collection and processing of location data should be limited to what is necessary to achieve the purpose(s) of gathering the data;
- Location data should be gathered only for the provision of the specified service and not be processed in ways that are incompatible with the provision of the service;
- Security measures should be implemented to protect location data from unintended or unauthorised disclosure;
- Data subjects should be informed of processing of location data on them.

⁵ Although the processing of location data contained in the traffic data and location data other than traffic data are handled separately in the directive, the explicit consent of the use is required for the processing both traffic data and location data.

It can be observed that these same principles can be easily found in the Data Protection Directive and even from the national data protection laws. For example, the Finnish Personal Data Act mentions explicitly necessity principle and the exclusivity of purpose among the main principles of the Act. Due to the New Tele Privacy Directive, an additional principle of informational self-determination should be added to the list:

- In relation to a provider of telecommunications service or a value added service, location data may be processed only with informed consent of the user, such consent possible to be withheld at any time

In the following chapter it is assessed how these principles could be reflected in the provision of location-based services.

3. *Location-based Services in the Light of general Data Protection Principles*

3.1. Understanding Location Data and Positioning Technology

Within the Navi Programme location data has been defined to refer to a location of an object in a reference system, such as a coordinate system. This broad definition of location data embraces large amounts of data. For example, address of a person or of a place of business is clearly a location data defining the location of an object with respect to an address system. Examining such a broad definition of location data would not be useful in this report.

For the purposes of this report location data is understood to refer to a location of a mobile terminal equipment, whether real-time location or location in a certain definite earlier moment. Mobile terminal equipment usually being carried by a person identifiable by a teleoperator, location of terminal usually defines also the location of the user of that terminal, and is such personal data of the user of the terminal (or of the user of the terminal known to the teleoperator) as well as of the subscriber of the mobile subscription.

As described in the Current Regulatory Framework –report, there are several methods for determining location data of a terminal equipment. 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, such as the assisted satellite navigation. In terminal-based positioning location data is originally in the control of the user. Such terminal equipment could be, for example, a mobile phone with GPS-chip attached.

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 network operator.

The distinction between terminal-based positioning and network-based positioning is important in many respects. It also affects our analysis of the general data protection principles.

3.2. The Role of a Teleoperator as a Trusted Party

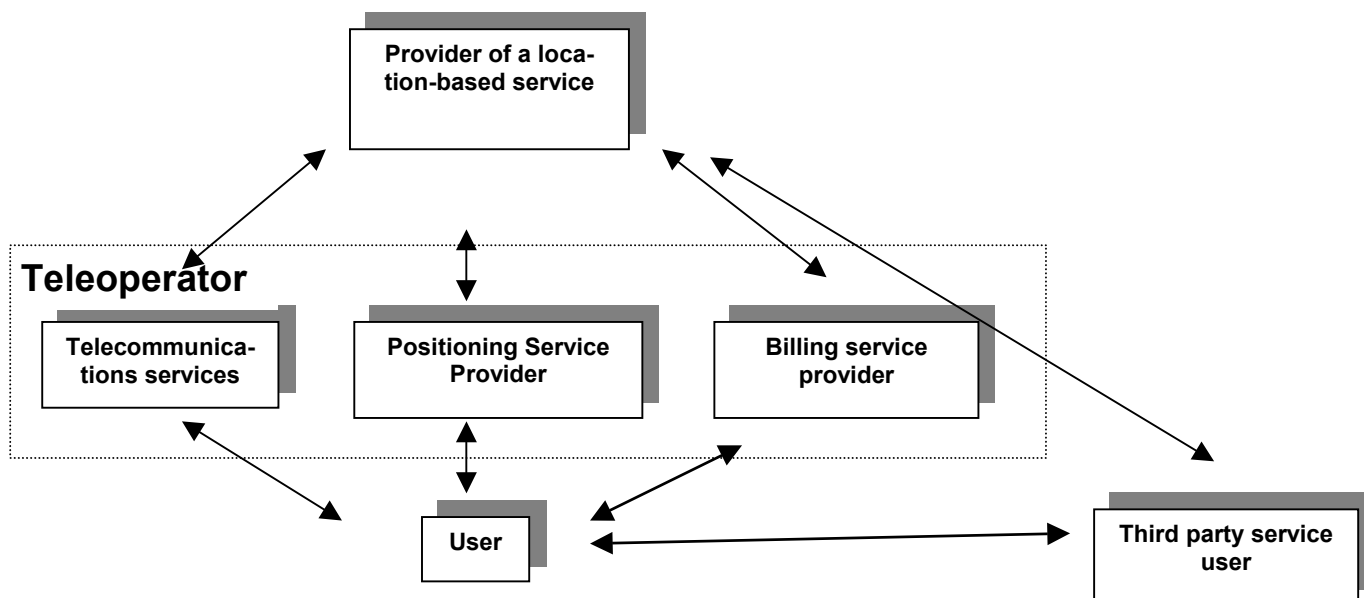
From privacy point of view, the main differences between network-based positioning and terminal-based positioning is the very fact that in the terminal-based positioning the user is the actor in control of the location data in the first place. In principle the location data is thus not disclosed to Service Providers or teleoperators unless the user knowingly does so. However, in practise the matter is somewhat more complicated. One widely discussed privacy risk related to the use of internet has been software applications sending personal information to internet without the consent of the user. Software may, for example, send information to the manufacturer of the software about the use patterns of the user. Similarly, a user of a mobile terminal might not always be aware of information that is being sent out from the terminal, for example attached to a service request.

It is clear the terminal-based positioning enables privacy friendly application more easily than network-based positioning. However, from the point of view of general data protection principles, division of the technology into terminal-based positioning and network-based positioning seems not to be all that relevant as it first appears: both technologies can be used in a way enhancing the fulfilment of the general data protection principles defined above, and both technologies has its drawbacks.

A couple of remarks should be made about the role and position of teleoperators. Due to their role as the controllers of the network, teleoperators necessarily have access to any information (unless it is encrypted at the terminal) distributed over communications networks, be it internet, GSM network or any other network. Thus teleoperator has a role of a trusted party that has access to certain information, but is trusted not to misuse such information. That role of a teleoperator is further underlined by industry-specific legislation in force in most countries prescribing detailed regulations about how to utilise such data and setting forth harsh penalties for misuse of such data.

It can be asked how location data differs from any other data processed by teleoperators. Teleoperators process large amount of sensitive data concerning contents of communications and traffic data relating to communications. In fact, teleoperators do continuously process location data of mobile terminal user in order to enable the very functioning of mobile communications. It can be argued that utilising location data for the provision of location-based services would not bring anything new to the situation.

3.3. Actors in the Provision of Location-based Services



In the picture above the typical actors in the provision of location-based service are presented. In this case it has been assessed that a network-based positioning is used. Teleoperator usually has multiple roles, taking care of communications services, positioning and billing. Provider of a location-based service then provides the service. The provision of the service usually involves delivery of information or other content to the terminal of the user or a third party service user. For example, in a find-a-friend –service, the location of the user is delivered to the third party service user.

In the presented location-based service the user has two customer relationships: one with the teleoperator concerning the subscription of the connection, one with the provider of the location-based service (Service Provider). These both parties, teleoperator and the Service Provider must fulfil the data protection principles set forth earlier in the report:

- Collection and processing of location data should be limited to what is necessary to achieve the purpose(s) of gathering the data;
- Location data should be gathered only for the provision of the specified service and not be processed in ways that are incompatible with the provision of the service;

- Security measures should be implemented to protect location data from unintended or unauthorised disclosure;
- Data subjects should be informed of processing of location data on them.
- In relation to a provider of telecommunications service or a value added service, location data may be processed only with informed consent of the user, such consent possible to be withheld at any time

Thus, neither party should process location data more than is required for the purpose, location data should not be used for any other purpose, sufficient security measures should be adopted, users of terminal should be informed of the processing of location data, and the user should give their explicit consent to the processing of location data for both parties.

From the above-mentioned requirements, the security obligations, informing obligations and consent are examined in more detail.

3.4. Security Obligations

It was concluded above that under the general data protection principles the teleoperator and the provider of location-based service should especially take care of the security of the data processing. What would such data processing contain in detail?

In the provision general telecommunications services teleoperators have implemented rather extensive security measures. Such measures have been implemented partly due to the express requirements of law. Location-based services being in many ways related to the telecommunications services, it could be argued that the same level of security should be applied.

In fact, the New Tele Privacy Directive, includes express security obligations the cover location-based services as well as other telecommunications services. In this respect it could be argued that the requirements of the general data protection requirements have been fulfilled, provided naturally that the security requirements set for the telecommunications sector in general are sufficient.

3.5. Consent and Informing in the Context of Location-based Services

We have concluded above that processing of location data requires an explicit consent of the user. The question arises what is considered sufficient consent for processing of location data. This question has been studied in more detail in the report Current Regulatory Framework.

Requirements of the Data Protection Directive are applied in interpretation of the consent given by the user for processing of location data. According to the directive the consent must be conscious. Furthermore, the consent must be also sufficiently detailed. 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 directive. The question remains naturally, what would constitute such a consent.

It is evident that a consent given by the user must always include the definition of the purpose of the processing for which the consent has been given. A mere consent without clarification of the extent of the consent could not be sufficient. Thus prior obtaining the consent, the user must always be informed of the purpose of the processing and of the extent of the processing. The consent cannot be obtained without sufficient informing. We can see that obtaining consent is thus closely intertwined with informing the data subject, and the question of sufficient consent to large extent boils down to the question of sufficient provision of information. In the following chapter the extent of the informing requirements are examined.

A final point about the consent is, that formally, under the general data protection principles both teleoperator and the Service Provider need a consent of the user to comply with their own customer relationship with the user (or with the subscriber, if not the same). Both teleoperator and the Service Provider have a separate customer relationship with different terms and obligations. This does not imply that the consent could not be acquired simultaneously, with one declaration of intent of the user. In fact, if the user has given its clear consent to teleoperator or the Service Provider, it does not seem likely that a separate confirmation would be required for other party. The proposed Finnish implementation of the New Tele Privacy Di-

rective takes this into account by stating that the teleoperator may obligate the Service Provider to acquire the consents needed.

3.6. Obligations Related to the Provision of Information

Questions related to different ways of providing information to the terminal user have been studied in more detail in the Current Regulatory Framework –report.

As noted above, consent is closely intertwined with the provision of information. In some situation this is also vice versa: it can be argued that a consent could in principle constitute a knowledge of the user about the nature of the service.

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 Provider ask for confirmation for the use of location data with a delivery of more detailed information of the processing of location data? The user must be aware of the processing of the location data for determining what map should be delivered to him, and if this is how the location data is actually processed, the user can be interpreted to already possess the required information.

It is difficult to argue that a mere order of a service would include a sufficiently informed, unambiguous, detailed and conscious expression of will for processing of personal data. However, in this kind of kind of situations where the very nature of the service is based on the positioning, the implied consent of the user might not be too far fetched. Compared to contractual law, implied contracts included considerably less-evident contractual terms have been held valid under several jurisdictions, provided that the contractual terms are not unfair or surprising.

Thus it could be argued that in some case an order from the user could even satisfy certain requirements on provision of information.

Generally speaking alternatives for explicit provision of information would be to deliver the information to the terminal of the user or make such information available, for example, at the web pages of the Service Provider. In practise it will probably any way be necessary to provide certain information concerning the services in other sources, such as in a web page of the Service Provider. However, it can be argued that provision of required information only on the web pages fulfils the criteria of general data protection principles only in relation to a service about which the user should have on the basis of the nature of the service a sufficient understanding, implying that the user should also be aware of the extent of the processing of the personal data in relation to such service. This is because the information available at the web page does not necessarily ever reach the user, and if the processing of location data is not reasonably evident in the context, the user will not be aware of the processing of location data. Thus it could also be argued, that making required information available separately from the ordering of the service should be allowed only in cases where the user should already have, on the basis of the nature of the service, a reasonable knowledge of the extent of the processing of location data.

Above were have merely discussed the provision of information when ordering the service. The New Tele Privacy Directive emphasises this information provided when the service is ordered. It should be noticed that the obligation of the Service Provider to inform the user of the processing of personal data does not end after the service has been ordered. From the point of view of general data protection principles the Service Provider should continuously inform the user of the changes in the processing of personal data, or even in some cases of the continuation of the processing of personal data. Such information obligations naturally depend on the nature of the service, but especially continuous services enabling tracking by third parties could be seen as services where continuous (for example weekly) reminder of the service could be well-founded. This, however, is an obligation that would be extremely difficult to be successfully implemented in legislation, since the nature of the services differ enormously.

3.7. Controller and Processor and the processing of Location Data

One further point arising out of the general data protection principles is that of the controller and processor of personal data. These concepts have been central in the data protection ever since the 1970s.

In the Data Protection Directive controller is defined as follows:

“the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data;...”

Processor of personal data is defined as follows:

“a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller”.

In short: the controller is the actor who determines the purposes and means of the processing of personal data, and processor is an actor processing personal data on behalf of the controller on the basis of, for example, an assignment. The idea stems from the earlier times of large central computers processing centrally large amounts of personal data. The idea of controller is very practical in many situations. However, in relation modern information technology application the concept of controller is not always very suitable.

In case of location-based services, a typical situation involves a service provider offering a location-based service that is entirely dependent on the activities of the user of a third party service user (as defined in the picture above). The Service Provider does determine the means of the processing of location data. Location data is processed only at the request of the user of the third party service user. The Service Provider is thus not the initiator of processing. It can be asked, whether in this kind of situation, where the control of the use of the location data is – or should be – entirely in the hands of the user or of the third party service user, the controller is actually the user or the third party service user, not the Service Provider.

Indeed, one way to approach the situation of location-based services would be to see the user of a mobile terminal as the controller of location data. The controller, the party having legal control over the processing of location data, would then give assignment to a teleoperator or a Service Provider to process location data for the provision of a location-based service.

This kind of approach underlines the informational self-determination of the terminal user with respect to the use of location data. This would in many (but certainly not in all) cases provide a better understanding of the legal positions of the part. This approach would also lower the difference between terminal-based positioning and network-based positioning, as the user's role as the processor of data is more easily seen in terminal-based positioning. It should be also noted that the Service Provider would anyway in most cases process some personal data, and possibly even location data, as a controller for the purposes of billing and certain other similar purposes.

It could be argued that this approach would not reflect the actual situation because the terms of the use of the data are in practise exclusively determined by teleoperator or the Service Provider through their control over the nature of the service and the applicable contractual terms. However, the situation could be compared to that of a company procuring, for example, mailing services from a service company under the general terms and conditions of the service company. The processor, the service company, would define the terms of the relationship through its general terms and conditions, but anyhow the assignor would be clearly deemed to be the controller of the personal data processed by the service company.

The present legal structure does not seem to give away to the approach of user as the controller of his own data. It is explicitly stated in the recital 47 of the Data Protection Directive that the teleoperator shall be considered to be the controller:

Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

The user is naturally understood to be the controller of the personal data contained in the message. However, the teleoperator is considered to be the controller of additional personal data necessary for the operation of the service. With respect of basic telecommunications services this might be a well-founded interpretation. Indeed, teleoperator is processing personal data that is used for the purposes of the teleoperator, i.e. for the maintenance of the customer relationship. For example, teleoperator is using personal data for the billing, and teleoperator is not depended on the consent of the user for such processing. The extent of the use of such data is largely defined by the teleoperator within the limits of applicable regulations.

It can be concluded that in the provision of normal telecommunications services teleoperator is clearly acting as a controller of the data. However, the interpretation of the terminal user as the controller of location data and other traffic data in relation to the provision of value-added services has some relevance. It could be argued that when asking the utilisation of location data for location-based services the user is actually taking the control for the use of such location data, such location data becoming comparable to a content of a message sent by the user.

4. Conclusions

In this report we have attempted to find a new approach to the provision of location-based services: that of common general data protection principles found in the European data protection regimes.

It can be concluded that certain main data protection principles applicable to the location-based services can be found. However, such principles are already clearly present in the existing legislation, and do not bring clarification to the roles or obligation of the actors. Thus it can be concluded (with some reservations) that existing industry-specific regulations for the location-based services fulfil the general data protection principles. This is not surprising, as *the very nature of data protection regulations is often that of general principles* governing the processing of personal data. Even in the level of national legislation the interpretation of these general principles is left to the public, the legislator does not provide the answers. This approach renders the data protection regulations flexible and adaptable to new circumstances.

However, it makes the interpretation of the data protection regulations very difficult, which, in turn, makes compliance with the regulation more difficult and diminishes legal certainty.

The role of teleoperator or a Service Provider as the controller of personal data can be questioned in the provision of value-added services. It could be argued that in this kind of situation it is actually the user of the mobile terminal who is the controller of the data, utilising such data for his/her own purposes.

As a final point it is noted that a “personal freedom” –point of view of general privacy principles could be another useful point of view for the analysis of the effect of monitoring and surveillance applications.