



PRIVACY & SECURITY LAW



REPORT

Reproduced with permission from Privacy & Security Law Report, 8PVLR24, 06/15/2009. Copyright © 2009 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

E-Commerce

EU Data Protection

Location Based Services: European Data Protection Rules for Mobile Commerce

By JORG HLADJK

I. Introduction

Wireless systems and unique identification of communication devices, combined with location data, enable service providers to deliver services based on location information. Information services that use the localization of the user via mobile network cells or satellites, in order to offer the user services that are tailored to its precise geographic position (so-called "Location Based Services" (LBS)), are among the most attractive services of mobile commerce. Examples of such services include; navigation services (tourist offers, management of car fleets or sales representatives, etc.); computer games and other games that make use of the possibility to locate the player (scavenger hunt, quiz, etc.); information services (weather, leisure time, restaurants, shopping, etc.); as well as advertisements (vouchers, etc.).

According to a study published in April 2008, revenue from LBS is forecast to reach an annual global total of

\$13.3 billion by 2013, up from an estimated \$515 million during 2007.¹ Furthermore, personal navigation and enterprise services are projected to be the highest revenue-generating services and are forecast to be worth approximately \$4.3 billion and \$6.5 billion respectively, per annum, by 2013. In addition, the survey shows that LBS will grow significantly in Europe and Asia. According to a July 2008 study, North America generated 81 percent of the world's Location Based Services revenue in 2007. By 2013, that percentage is expected to decrease to just 32 percent. In the same period, Western and Eastern Europe's combined LBS revenues will jump from just 5 percent to 31 percent. The Asia-Pacific region, meanwhile, will see a rise from a 2007 share of 11 percent, to 27 percent.²

Depending on the technical set up, LBS can be divided into direct and indirect provisions of services. A service can be provided either directly by the telecommunications provider (the individual concerned contacts the telecommunications provider, who then provides the service on the basis of the location data obtained from his system) or via a third party content provider (the individual concerned contacts a content

Dr. Jörg Hladjk, with Hunton & Williams LLP, Brussels, can be reached at jhladjk@hunton.com.

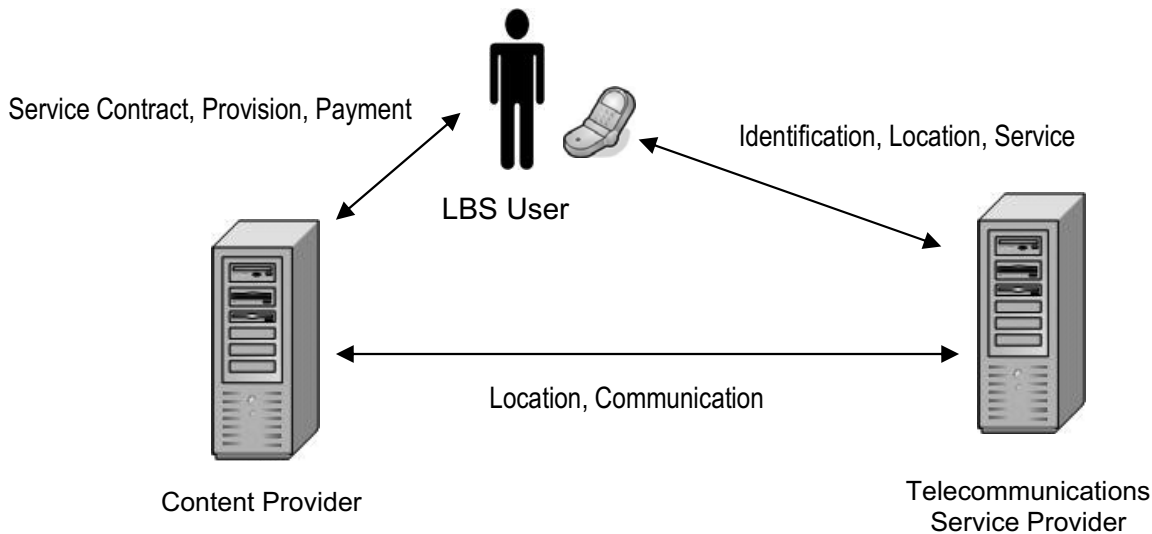
¹ ABIresearch, Mobile Location Based Services Revenue to Reach \$13.3 Billion Worldwide by 2013, April 3, 2008.

² ABIresearch, Location Based Services "On the Move" in Asia and Europe, July 2, 2008.

provider, who then provides the service on the basis of the location data obtained from the telecommunications provider).

tronic communications sector. In addition, the EU Data Protection Directive⁶ (also referred to as the “General Data Protection Directive”), which sets forth the funda-

Parties involved in a Location Based Service:



While these services are very attractive from a commercial point of view, they raise significant concerns under European data protection law, because the users are under constant observation and can be located at any time. This brings the risk that the location data generated can be used to create comprehensive and meaningful user profiles about behavior and movements. Several studies indicate that users are concerned about the unsolicited use of personalized location data, and that control over personal data is an important criterion for users when selecting location based services.³ The studies also conclude that the employment of technical measures that would allow users to control their personal data would lead to greater acceptance of LBS.⁴ The following sets out the legal framework for providing LBS in Europe.

II. Applicable laws

LBS providers are faced with various relevant laws, at both European and Member State levels. On the European level, the European Directive on Privacy and Electronic Communications (the so-called “e-Privacy Directive”)⁵ is concerned with the processing of personal data and the protection of privacy in the elec-

mental rules of data protection, is also applicable. The e-Privacy Directive contains specific rules and particularizes and complements the General Data Protection Directive for the purposes mentioned.

In addition, the national laws of the Member States have to be taken into account, since each Member State has implemented the Directives differently and it is national law, not EU law, which determines the details of compliance. In Germany, for example, this would include the Telecommunications Act (*Telekommunikationsgesetz*)⁷, the Telemedia Act (*Telemediengesetz*)⁸ and the Federal Data Protection Act (*Bundesdatenschutzgesetz*)⁹. Location data generated by a mobile phone service provider (responsible for the “transport” level of the data) via a LBS are subject to the rules on confidentiality of communications under the Telecommunications Act, whereas the provider of the concrete LBS (content or added value level) has to comply with the special data protection provisions of the Telemedia Act. When such laws do not provide special rules for the use of the data, the general, subsidiary, rules of the Federal Data Protection Act will be applicable. Although all

³ See for example: Barkhuus/Dey, Location-Based Services for Mobile Telephony: a study of users’ privacy concerns; http://www.itu.dk/~barkhuus/barkhuus_interact.pdf, Hahn/Fritsch, Studie zur Akzeptanzanalyse von Location-Based Services; http://publikationen.ub.uni-frankfurt.de/volltexte/2005/2300/pdf/StudieLBSAkzeptanz_Hahn2005.pdf, p. 9

⁴ Fritsch/Muntermann, Aktuelle Hinderungsgründe für den kommerziellen Erfolg von Location-Based Service-Angeboten, <http://www.wiwi.de/publikationen/AktuelleHinderungsgruendefuerden1160.pdf>, p. 12 and 14.

⁵ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic com-

munications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37 - 47.

⁶ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31 - 50.

⁷ Telecommunications Act of 22 June 2004 (BGBl. I S. 1190), as amended by Article 3 of the Act from 25 December 2008 (BGBl. I S. 3083).

⁸ Telemedia Act of 26 February 2007 (BGBl. I S. 179), as amended by Article 2 of the Act of 25 December 2008 (BGBl. I S. 3083).

⁹ Federal Data Protection Act of 14 January 2003 (BGBl. I S. 66), as amended by Article 1 of the Act of 22 August 2006 (BGBl. I S. 1970).

these laws are to a great extent based on the same principles, such as data minimization, primacy of the right to informational self-determination over the service provider's commercial interests, transparency and data security, etc., the wording used in the various laws and the obligations imposed upon the service providers may differ significantly.

III. Use of location data

In order to determine the legal framework for the use of location data, it is important to define "location data" under the European legal framework and how this relates to LBS. According to the e-Privacy Directive, "location data" means 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.¹⁰ Further details can be found in the recitals of the Directive, according to which 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, and to the time the location information was recorded.¹¹ In addition, "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.¹²

While LBS services are very attractive from a commercial point of view, they raise significant concerns under European data protection law.

The e-Privacy Directive further regulates the processing of location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services for the provision of a "value added service."¹³ "Value added service" means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof.¹⁴ Such "value added services" may, for example, consist of advice on route guidance, traffic information, weather forecasts and tourist information.¹⁵ LBS are thus a type of value-added services.

The rules outlined above mean that location data may or may not constitute "traffic data." Therefore, location data can be divided into two categories. First, the processing of location data which are a by-product of the communication service and constitute traffic data. Such data is governed by Article 6 ("traffic data") of the e-Privacy Directive. A later use of this type of location data for LBS, is, however, not legitimized by Article 6 of the e-Privacy Directive. To assess the lawfulness of the

use of location data for LBS, one has to consider Article 9 ("Location data other than traffic data") of the e-Privacy Directive. It states that location data other than traffic 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.

1. Requirement of consent

The processing of location data for the provision of value added services is subject to the prior consent of the subscriber or of the user. The e-Privacy Directive states in recital 31 that "whether the consent to be obtained for the processing of personal data in order to provide a particular value added service should be the user's, or the subscriber's, not only depends on the data to be processed and on the type of service to be provided, but also 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."

According to the e-Privacy Directive, a "user" means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service.¹⁶ The requirements regarding consent to be provided by the subscriber or the user are the same as those specified in the General Data Protection Directive, according to which "consent" means any freely given specific and informed indication of wishes by which the individual signifies its agreement to personal data relating to him being processed.¹⁷ Consent may be given by any appropriate method such as ticking a box when visiting an internet Web site, as long as it is a freely given, specific and informed indication of the user's wishes.¹⁸

In some Member States, telecommunications law contains specific requirements concerning electronic consent. For example, in Germany, the provider must ensure that: (1) the subscriber or user has given consent deliberately and unequivocally; (2) consent is recorded; (3) the subscriber or user can access his declaration of consent at any time; and (4) the subscriber or user can withdraw his consent at any time with effect for the future.¹⁹

Consent may be given for any individual use of location data or by an overall consent for a variety of similar uses, for example if a framework agreement has been concluded between the service provider and the user.

2. Right of withdrawal of consent

In addition, the user or subscriber must be given the possibility to withdraw consent for the processing of location data other than traffic data at any time.²⁰ This not only requires that the user or subscriber has the right to withdraw consent at any time, but also that they are given the effective possibility to do so. Withdrawal also prohibits the service provider from processing the customer's data in the future. Therefore, the provider must ensure that it has the appropriate mechanisms in

¹⁰ Article 2 c) of the e-Privacy Directive.

¹¹ Recital 14 of the e-Privacy Directive.

¹² Article 2 b) e-Privacy Directive.

¹³ Article 9 of the e-Privacy Directive.

¹⁴ Article 2 c) of the e-Privacy Directive.

¹⁵ Recital 18 of the e-Privacy Directive.

¹⁶ Article 2 a) of the e-Privacy Directive.

¹⁷ Article 2 h) of the General Data Protection Directive.

¹⁸ Recital 17 of the e-Privacy Directive.

¹⁹ Section 94 of the German Telecommunications Act.

²⁰ Article 9 para. 1, 3rd sentence of the e-Privacy Directive.

place to show whether or not consent has been withdrawn and to take appropriate action if a customer decided to exercise this right.

3. Right of temporary refusal of processing

Further, the e-Privacy Directive states that when a user or subscriber has given consent to the processing of location data other than traffic data, the user or subscriber must still continue to have the possibility of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.²¹ With regard to the modalities of the refusal process, the Directive only specifies that such temporary refusal must be free of charge and should be rendered possible by the use of a simple means. However, the Directive does not indicate whether the refusal should apply per connection or transmission, or over a certain period of time.

4. Information to the subscriber or user

The service provider must inform the users or subscribers, prior to obtaining their consent, of (1) the type of location data (other than traffic data) which will be processed, (2) the purposes and duration of the processing, and (3) whether the data will be transmitted to a third party for the purpose of providing the value added service.²² The information should be provided prior to the consent given by the user or the subscriber for the use of its data, either for marketing purposes or for the provision of value added services. In case the provider does not sufficiently inform the user prior to the consent being given, the consent is considered to be invalid and any collection, processing and use of the location data is unlawful.

5. Restricted data processing

The e-Privacy Directive states that the processing of location data other than traffic data should be restricted to personnel acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and that the processing must be limited to what is strictly necessary to provide the value added service.²³ Therefore, it is prohibited for a provider of a value added service to process location data (other than traffic data) for the purposes of promoting its services, which, on the contrary, is allowed under Article 6 of the e-Privacy Directive for the processing of traffic data. This is an important difference between the two categories of data that needs to be observed when processing location data.

6. Transfer to third parties

The e-Privacy Directive impliedly allows for a possible transfer of location data other than traffic data by the service provider to other parties. Actually, a provider of value added services is mentioned as one of the specific categories of service providers under the authority of which location data other than traffic data may be processed.²⁴ Such processing involves the transfer of location data other than traffic data from the provider of the public communications network or the

publicly available communications service. Moreover, the e-Privacy Directive expressly foresees the forwarding of location data to a third party providing value added services by requiring that the subscribers or users to whom the data are related be fully informed of the forwarding of the location data before giving consent to its the processing.²⁵

7. Subcontracting of services

The issue of subcontracting part or all of the processing of traffic data carried out by the service provider to a processor in the sense of the General Data Protection Directive²⁶ is not dealt with in the e-Privacy Directive. The e-Privacy Directive only deals with the processing of location data other than traffic data by persons “acting under the authority” of the service provider (see above, under 6.). The wording “acting under the authority”²⁷ of a data controller does not seem to constitute an authorization to subcontract the processing to a data processor. Recital 32 of the e-Privacy Directive, however, seems to explicitly allow such subcontracting. It states that where the provider of an electronic communications service or of a value added service subcontracts the processing of personal data necessary for the provision of these services to another entity, such subcontracting and subsequent data processing should be in full compliance with the requirements regarding controllers and processors of personal data as set out in the General Data Protection Directive.

Therefore, subcontracting of location data processing by an electronic service provider or by a value added service provider is permissible, under certain conditions. For example, a provider of telephony services could provide location data to a third company in the framework of a processing agreement to provide end customers with weather forecast or tourist information based on their location data. In such a case, however, the service provider is required to inform the users and subscribers about the forwarding of their location data before they give their consent to the processing the data for the provision of the value added services.

IV. Consequences of the illegal use of location data

The e-Privacy Directive does not provide for sanctions in case of illegal use of location data, but national telecommunications law in some Member States does provide for such sanctions. In Germany, for example, the illegal processing of location data would constitute an administrative offense punishable by way of a maximum fine of €300,000 (\$416,864).²⁸ Further, the German Telecommunications Act provides that the fine should exceed the economic benefit the offender has derived from the offense.²⁹ In addition, the user has the right to request at any time information about the data

²⁵ Recital 32 of the e-Privacy Directive.

²⁶ Article 17 para. 2 and 3 of the General Data Protection Directive.

²⁷ See Article 9, para 3 of the e-Privacy Directive.

²⁸ See section 149 para. 1 and 2 of the German Telecommunications Act.

²⁹ See section 149 para. 2 of the German Telecommunications Act.

²¹ Article 9, para. 2 of the e-Privacy Directive.

²² Article 9, para. 1, 2nd sentence of the e-Privacy Directive.

²³ Article 9, para. 3 of the e-Privacy Directive.

²⁴ Article 9, para. 3 of the e-Privacy Directive.

used.³⁰ If the data has been stored and used illegally, the user can bring a claim for injunctive relief, request correction, deletion or blocking of the data as well as bring a claim for damages.³¹

Finally, the provider should consider that a violation of data protection law may also constitute a violation of the German Unfair Competition Act, and competitors and consumer protection associations may therefore be entitled to bring actions against the provider because of the offence.³² This may lead to additional claims of injunctive relief, damages and/or disclosure obligations.³³ Therefore, the consequences of illegal processing of location data may go beyond those of just data protection law.

V. Security of location systems

With regard to data security, service providers need to ensure that they protect location data in location systems appropriately. This especially applies to location data corresponding to individuals such as customers or subscribers. As already described, location systems typically use IT systems, at least in the backend, to store and process location data.

1. Obligation to implement security measures

The e-Privacy Directive imposes security obligations on the service providers due to the specificity of the risks associated with the use of networks. According to the e-Privacy Directive, the service provider must take appropriate technical and organizational measures to protect the security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security.³⁴

The processing of location data for the provision of value added services is subject to the prior consent of the subscriber or of the user.

The concept of “security” under European data protection law is quite broad. According to the General Data Protection Directive, it means protection of personal data, such as location data, “against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.”³⁵ For example, the interception of the service by unauthorized third parties requires appropriate protec-

³⁰ See section 93 sentence 4 of the German Telecommunications Act and Section 34 of the German Federal Data Protection Act.

³¹ See sections 6, 7 and 35 of the German Federal Data Protection Act.

³² See for example Hellmich, *Location Based Services - Datenschutzrechtliche Anforderungen*, *Multimedia und Recht*, 2002, p. 157.

³³ See also Schmitz, in Schuster, *Vertragshandbuch Telemedia*, 2001, p. 187; see also OLG Köln (Higher Regional Court of Cologne), *Beschluss vom 9.4.1999*.

³⁴ Article 4, para. 1 of the e-Privacy Directive.

³⁵ Article 17, para. 1 of the General Data Protection Directive.

tions such as encryption or the use of otherwise secured networks or lines as well as implementation of fire walls. The legal requirement is not limited to technical measures, but also includes organizational measures, such as, for example, the appointment of a data security officer who is qualified to ensure compliance of the service with the relevant provisions of the Data Protection Directives. In addition, it may be necessary to coordinate the security efforts with the network provider to ensure protection, e.g. by blocking automatically any access to the system of the service provider.

With regard to the level of security, the Directive requires that any security measures have to ensure a level of security appropriate to the risk presented, but also should take into account the state of the art and the cost of their implementation.³⁶ Therefore, the provider needs to consider the potential risks associated with the nature of the service regarding both the likelihood of its occurrence and the harm that would result. “State of the art” in this context means in particular the security standards developed by standardization organizations such as ISO [International Organization for Standardization]. These standards can be classified in product-related and procedure or organization-related standards. In the context of products the Common Criteria (CC; ISO/IEC 15804) are of particular importance. They allow the definition and certification of the so-called security functions a product offers, such as encrypted storage of data, effective access control mechanisms, etc. For the implementation and operation of IT systems typically Information Security Management Systems (ISMS) are used. Based on the results of a risk analysis, technical and organizational security measures are used in combination to reduce risks until they are acceptable for the organization. To ensure the effectiveness and appropriateness of the selected measures in running operations of IT systems, a process based IT Security Management is used. ISO/IEC 27001 offers “good practice” examples for ISMS. For technical security measures, classifications (e.g. ISO/IEC 17799) and catalogues (e.g. the Baseline-Protection-Catalogues offered by the German Federal Office for Information Security) are available. The more significant the risk, the higher the security level that must be achieved considering cost of implementing measures. In addition, the e-Privacy Directive emphasizes the obligation of the service provider to adapt continuously the level of security taking into account the evolution of the state of the art.³⁷ Therefore, providers should review security measures on an annual basis to ensure appropriate measures are applied.

2. Obligation to inform subscribers

The e-Privacy Directive also requires that in case of a particular risk of a breach of the security of the network, the service provider must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies including an indication of the likely costs involved.³⁸ For example, in case of failures in the security of the system or any attacks by hackers, the provider has the duty to provide infor-

³⁶ Article 17, para. 1 of the General Data Protection Directive.

³⁷ Recital 20 of the e-Privacy Directive.

³⁸ Article 4, para. 2 of the e-Privacy Directive.

mation about the existence of these risks. In case no actions are available for the provider to avoid the risk, it must alert the subscriber about the possible ways of avoiding the risk including the costs of these remedies. The provision may qualify as an example for the reversal of the burden of proof. At the time this article was finalized, the relevant provision in the e-Privacy Directive was under review by the European Commission to include a security breach notification requirement in case of actual breaches, not just a “risk.” The proposed requirement would mean that providers would have to notify the competent national authority and/or individual about the breach under certain circumstances.³⁹

VI. Data retention

According to the e-Privacy Directive, location data other than traffic data may be processed only for the duration necessary for the provision of a value-added service.⁴⁰ This means that once the service has been provided, the service provider may not, in principle, store an individual’s location data, unless they are needed for billing and interconnection payment purposes.

Directive 2006/24/EC⁴¹ on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (so-called Data Retention Directive), that amends the e-Privacy Directive, contains more specific rules with regard to the retention of location data. The Data Retention Directive regulates the mandatory storage of traffic and location data on both legal entities and natural persons and of the related data necessary to identify the subscriber or registered user. It does not, however, apply to the content of electronic communications, including information consulted using an electronic communications network.⁴² The data need to be stored by service and network providers in order to ensure that the data are available for the purpose of the investigation, detection

³⁹ See Draft Recommendation for second reading on the Council common position for adopting a directive of the European Parliament and of the Council on amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities for the enforcement of consumer protection laws (16497/1/2008 – C6-0068/2009 – 2007/0248(COD)), March 4, 2009, p. 58/59 and the European Parliament legislative resolution of 6 May 2009 on the common position adopted by the Council with a view to the adoption of a directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (16497/1/2008 – C6-0068/2009 – 2007/0248(COD)).

⁴⁰ Article 9, para. 1 of the e-Privacy Directive.

⁴¹ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105 , 13/04/2006 p. 54 - 63.

⁴² Article 1, para 2 of the Data Retention Directive.

and prosecution of serious crime, as defined by each European Member State in its national law.⁴³

By way of derogation from the e-Privacy Directive, the Data Retention Directive states that these data must be retained to the extent that they are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.⁴⁴ The data to be retained are specified in the Data Retention Directive, which distinguishes between fixed and mobile telephony on the one hand, and Internet e-mail and Internet telephony on the other. The obligation includes unsuccessful call attempts, i.e., where a telecommunications connection was made, but the call was not answered by the recipient, if such data are stored (as regards telephony data) or logged (as regards Internet data) by the provider.⁴⁵

According to the e-Privacy Directive, location data other than traffic data may be processed only for the duration necessary for the provision of a value-added service.

In the context of the provision of LBS, the data mentioned in Article 5 para. 1 (f) of the Data Retention Directive are particularly relevant. These are data necessary to identify the location of mobile communication equipment and have to be retained. This includes (1) the location label (Cell ID) at the start of the communication and (2) data identifying the geographic location of cells by reference to their location labels during the period for which communications data are retained.

The required duration of storage is at least six months with a maximum of two years. The exact period of storage is to be decided upon by each Member State in its implementation of the Data Retention Directive. The maximum period may even be extended, for a limited period, for EU Member States facing particular circumstances that warrant an extension. The Data Retention Directive had to be transposed in the EU Member States by Sept. 15, 2007, with a possible postponement for Internet data until March 15, 2009. At the time this article was finalized, not all Member States had implemented the Directive completely. Therefore, data retention programs for LBS have to be assessed on a case by case basis depending in the location of the service provider, and national law requirements have to be considered carefully.

VII. Provision of international services

In a global business environment, many value-added services are based on the processing of location data from electronic communications services, but are provided by companies (e.g. via a website) not established in the territory of the customer concerned. The e-Privacy Directive applies to the processing of per-

⁴³ Article 1, para 1 of the Data Retention Directive.

⁴⁴ Article 1, para. 1 of the Data Retention Directive.

⁴⁵ Article 3, para. 2 of the Data Retention Directive.

sonal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community.⁴⁶ According to the General Data Protection Directive, the applicable national law is that of the Member State where the provider of the value-added service is established. Further, when the same provider is established on the territory of several Member States, it must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by each national law applicable.⁴⁷ These latter provisions mean that, within the European Community, the processing of location data is subject to the national law of the Member State where the service provider is established and not the Member State of which the customer is a national.

Where the provider of the value-added service is not established in a Member State, the location data may be transferred from the electronic communications operator to the controller only on the terms laid down in the General Data Protection Directive on the transfer of personal data to third countries.⁴⁸ Such terms include the requirement that the data protection laws in the

third country be found adequate by the European Commission, or else that the transfer be based on other legitimating grounds such as the customer's consent or the existence of a contract concluded in the customer's interest.

VIII. Conclusion

The current legal framework for processing location data generated by location based services is highly complex. With three European Directives that partially overlap, LBS and each containing definitions of personal data, traffic data, and location data, it can be a challenging task to determine which legal provisions apply when providers of LBS process location data. In addition, a wide variety of LBS applications based on diverging technologies exists, the legal categorization of which can be difficult. Besides the complex legal issues, there are also practical issues that need to be considered when offering location based services. In view of the consequences, providers of location based services should pay special attention to the protection and legal framework of location based data. In particular, in order to ensure that any consent given will be considered valid, and therefore justifying the processing of location based data, the users should be adequately and comprehensively informed prior to giving their consent. The European legal consequences of location data processing thus need to be carefully considered in offering LBS.

⁴⁶ Article 3, para. 1 of the e-Privacy Directive.

⁴⁷ Article 4, para. 1 a) of the General Data Protection Directive.

⁴⁸ See Articles 25 and 26 of the General Data Protection Directive.