scripted

Volume 5, Issue 2, August 2008

Reasonable Expectations of Geo-Privacy?

Dr. Sjaak Nouwt [*]

Abstract

This article endeavours to highlight the technological developments for Location Based Services by governments in relation to the data protection rules and to the concept of privacy. The main question is whether the 'reasonable expectations of privacy' is a suitable concept for privacy protection in the context of geo-information about citizens. The use of modern positioning techniques makes it easy to collect and record geographical location information about people. As a result, time and place are now becoming important elements again whereas in the Internet era they were beginning to diminish. By using location information, governments are able to develop Location Based Services for their citizens. These services are especially interesting from a data protection and privacy perspective because when the services are not in compliance with the data protection and privacy rules, providing these services might be annulled by the courts. Data protection issues relating to location information follow from three European Directives regulating respectively data protection, privacy and electronic communications, and data retention. Where it seems rather easy to conclude whether data protection rules are applicable to location information, this does not appear to be so easy for the recognition of privacy. We shall discuss the 'reasonable expectations of privacy' and the privacy concept of Article 8 ECHR in that context. The question is, which one will provide enough guidance for the protection of geo-privacy?

DOI: 10.2966/scrip.050208.375

[*] Assistant Professor at TILT – Tilburg Institute for Law, Technology, and Society. Tilburg University, the Netherlands.

1. Introduction

The Tilburg Institute for Law, Technology, and Society (TILT) has been participating in an extensive Dutch innovation programme, entitled 'Space for Geo-Information' since 2006.[1] Under this programme the TILT-GEOGOV research group, together with computer scientists and political scientists, are participating in the research project called GEOGOV. This project particularly focuses on the use of spatial or geographic information (geo-information) by governments. The starting point for the GEOGOV project is that there is a need for a social scientific approach of the process, from the development of geo-applications to their implementation in society. More specifically, TILT concentrates on the legal and political aspects of governments using geo-information about their citizens to provide Location Based Services (LBS).

It is obvious that privacy and data protection are important issues to be considered when governments use geo-information about their citizens. Personal information enables governments to deliver LBS to their citizens. This article endeavours to highlight the developments of LBS by governments in relation to the data protection rules and to the concept of *'Reasonable Expectations of Privacy.'* This concept was introduced as a litmus test in 1967 by Judge John Marshall Harlan, a former member of the US Supreme Court. According to this test, a person can have a reasonable expectation of privacy when (1) he has an actual (subjective) expectation of privacy in a certain situation, and (2) society is prepared to recognise this (objective) expectation as reasonable (see also section 4.2).

This article deals with different types of data. The general context of this article is the protection of privacy and 'personal data.' 'Geographic data' becomes 'personal data' when it is related to an identified or identifiable natural person. When it provides information about locations of people we call this: 'location data.' Apart from location data, which in general provides information about where you are, it also deals with 'traffic data', which can provide information about where you have been. Traffic data is, for example, necessary for the conveyance and billing of mobile communications. Finally, 'movement data' can provide information about the route you (or your terminal equipment) have taken or about the duration of your movement.

This article also deals with different privacy concepts. 'Privacy' is a general concept and this article is more particularly about 'information privacy' or data protection. A more specific concept of privacy is the '*reasonable expectations of privacy*' concept. In this article, the concept of 'geo-privacy' refers to the protection of 'information privacy' with regard to geo-information.

This article is set-out as follows. In section 2, I will first explain the importance, meaning, and possibilities of geo-information. In this respect, I will also provide an overview of a number of positioning techniques that make it possible to generate geo-information. In section 3, I will explain how the European legal framework is applicable when geo-information can be related to individuals. More specifically, this legal framework consists of the general Data Protection Directive, the e-Privacy Directive, and the Data Retention Directive. In section 4, I will discuss the concept of

---

[1] Ruimte voor Geo-Informatie (RGI). Information about this program is available in English at *http://www.rgi.nl/?l=eng*. Information about the GEOGOV-project is available at: *http://www.geogov.eu/*.

'*reasonable expectations of privacy*', in particular with regard to geo-information collected in public places. I will explain that, according to European case law, we can also have reasonable expectations of privacy in public places. In section 5, I will conclude that the privacy concept of article 8 ECHR seems to provide more legal certainty and a better privacy protection than the concept of '*reasonable expectations of privacy*.'

2. Geo-information

2.1 The Importance of Time and Place

In the virtual world of electronic communications, like the Internet, time and place have become obsolete factors. At least, that is what we have come to believe for a number of years. However, it seems that we are now at a stage of 'reterritorialisation' where time and place are becoming important again.[2] Mobile communications by the Global System for Mobile Communications (GSM) or Universal Mobile Telecommunications System (UMTS) use a cellular based network architecture. The geographic area within which we communicate is divided into *cells*, varying from several meters to tens of kilometers. Such a geographic area is covered by a number of Base Transceiver Stations (BTS or *antennas*). A *cell* is the part of the area that is covered by one antenna. The area is divided into a number of overlapping uniquely identifiable *cells* by means of the *antenna*. The reach of one cell can vary from 100m in the city to 30 km in the countryside. For mobile communication to take place it is necessary to know the location of the cell phone. This is required to establish the communication and also for billing purposes. As a result, information is available about the geographic position where the user of a mobile phone equipment is at a certain moment. Therefore, time and place have again become important elements.

2.2 What is Geo-Information?

By using the concept of 'geo-information' several types of data can be covered. In this respect we will focus on geographic data, location data, and movement/mobility data.

Geographic data (hereafter referred to as geo-information) is "information describing the location and attributes of things, including their shapes and representation." Geographic data is the composite of spatial data and attribute data.[3] This data is related to a place on earth. Geo-information is for example the location of buildings, roads, and parcels in a landscape, combined with information about these objects, like the function of the building, the type of road, and the use of the parcel.[4] Other examples are the position of cables and wires in the subsoil, combined with

---

[2] See also: C van Ooijen, 'Territorialising eGovernment: A new perspective on the government-citizen relationship in the ICT-age?' Paper submitted to panel track 12: eGovernment and Institutional Change. XII Annual Conference of the International Research Society for Public Management, 26-28 March 2008, Brisbane, Australia.

[3] ESRI Online, GIS Dictionary *(http://support.esri.com*: Home > Knowledge base > GIS Dictionary)

[4] H Scholten, *Geografische Informatie Systemen*. Lelystad: IVIO uitgeverij, 2006. AO 2869, p. 6.

information about their functions and administrators. Borders are also geo-information, e.g. borders of parcels and borders of municipalities.

Geo-information is used by governments, the private sector, and by citizens.[5] In the public sector, geo-information is used for example by the land registry, meteorological institutes, and the ministry of transport (for example for road pricing). In the last two decades, the private sector has invested largely in creating geo-information databases and some well-known private businesses that have made that investment are: TeleAtlas, NavTeq, Google, Cyclomedia. And citizens are also increasingly using geo-information, for example to upload pictures to Google Earth or to use Google Streetview, navigate with TomTom or use it for vehicle tracking with GPS.

A legal definition of 'location data' can be found in the European Directive 2002/58/EC (Privacy and electronic communications), Article 2(c), where it describes location data as:

> *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.*

Preamble (14) of Directive 2002/58/EC explains that location data may refer to the latitude, longitude and altitude of the user's terminal equipment. Furthermore, it may also refer 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. Sometimes, the location of the terminal equipment of the sender or the recipient can also be called "traffic data." This is the case in digital mobile networks, when location data giving the geographic position of the terminal equipment of the mobile user are processed to enable the transmission of communications.[6] Location data is more precise than is necessary to enable the transmission of communications. They are very useful to deliver value-added services to the subscriber or user, like providing individualised traffic information and guidance to motorists.

Another category of geo-information is 'movement data' or 'trajectories.'[7] Movement data are data about changes in the physical position of an entity with respect to a reference system within which positions can be assessed. For example, geographical space is such a reference system. A trajectory can be described as the path made by the moving entity through the space where it moves. Such a path requires a certain amount of time. As a result, trajectories and time are inseparable. Trajectories relate to

---

[5] See also B van Loenen, J Zevenbergen, J de Jong, 'Geo-informatie: wat is het en wat is de juridische context?', in: L van der Wees, S Nouwt (eds.), *Recht en locatie. Geo-informatie in een juridische context.* Den Haag: Elsevier Juridisch, 2008, p. 11-33.

[6] 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 communications sector (Directive on privacy and electronic communications). *Official Journal* 2002, L 201/37, amended by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006. *Official Journal* 2006, L 105/54, preamble 35.

[7] See for example N Andrienko *et al*, 'Basic Concepts of Movement Data', in F Gianotti and D Pedreschi (eds.), *Mobility, Data Mining and Privacy. Geographic Knowledge Discovery*. Berlin – Heidelberg: Springer Verlag 2008, p. 15-38.

the movement of entities, like people, vehicles, or terminal equipment. Movement data can result in a route a person has taken or other characteristics of the movement, like the duration of the movement. Such information can also be of legal importance. In a famous Dutch murder case, the Court of Justice at 's-Hertogenbosch was of the opinion that on 23rd September 1999 at 8:36 p.m. the suspect made a phone call with his cell phone via Base Transceiver Station 14501 in the city of Deventer, which proved that at that time, the suspect must have been in or near the city of Deventer and not 24 kilometers away.

2.3 Location Services

To make things clear, the TILT-GEOGOV research group has divided geo-information into Geographic Information Systems (GIS) and Location Based Services (LBS). Because LBS are services meant for large groups of non-professional users (citizens, consumers, employees) and are based on the recent evolution of public mobile services, we will concentrate on LBS because these services often need personal data from their receivers in order to be able to deliver the service. Therefore, we think that privacy and data protection issues are more (although not exclusively) related to LBS rather than to GIS.

Location Based Services (LBS or 'Location Services') deliver information about location to people who are using wireless, position-aware devices such as cell phones and PDAs. LBS is defined as "Information or a physical service delivered to multiple channels, exclusively based on the determined location of a wireless device. Some location-based applications include emergency services, information services, and tracking services."[8]

LBS are also called Mobile Location Systems (MLS).[9] An MLS is defined as "a location system, including applications that determine the geographic position of mobile subscribers and provide them with relevant information and services." This definition illustrates that an MLS is associated with one or more positioning techniques (satellite-based or cellular-based, see also section 2.4) and that it supports the communication of information and services between the system and the subscriber.

Location data can be very important for emergency services to locate the caller of "112." In this respect, we refer to the "E112" service (location-enhanced 112): an emergency communications service using the single European emergency call number, "112", which is enhanced with location information regarding the calling user. "eCall" is an enhanced version of "E112" and is an electronic safety system that is in-built in cars and automatically calls the emergency services if the car is involved in an accident.[10]

---

[8] ESRI Online, GIS Dictionary. Available at: *http://support.esri.com*: Home > Knowledge base > GIS Dictionary (last modified October 31, 2006).

[9] C Renso et al, "Wireless Network Data Sources" in F Gianotti and D Pedreschi (eds.), *see* note 7, p. 83, with reference to G. Swedberg, Ericsson's mobile location solution. *Ericsson Review*, Issue no. 4/1999.

[10] European Commission, Information Society and Media, 'eCall - saving lives through in-vehicle communication technology.' General factsheet 49, July 2007. Available at: *http://ec.europa.eu/information_society/activities/esafety/doc/esafety_library/049_ecall_en.pdf*.

2.4 Positioning Techniques

In this section, a short overview will be presented of technologies that make it possible to generate location information. These technologies are also known as "positioning techniques."[11] These positioning techniques can be either cellular-based, satellite-based, or nonconventional.

Cellular-Based Positioning Technologies are for example, GSM and UMTS. A general description of these techniques was given in section 2.1. The most commonly used cellular positioning techniques are called Cell Identity (CI), Cell Identity and Timing Advance (CI+TA), Enhanced Observed Time Differences (E-OTD), and Assisted GPS (A-GPS). With CI, the location of a mobile device is identified by the cell to which it is connected. The accuracy varies from 100 meters to several kilometres. CI+AD improves CI by measuring the distance between the antenna and the mobile device. The accuracy is slightly better than CI, depending on the environmental conditions that can affect the strength of the signal, like high buildings and other obstacles. In the E-OTD positioning method, the handset measures the arrival time of signals transmitted from three or more antennas. The accuracy can vary from 50 to 100 meters. A-GPS is a simpler and cheaper positioning technique. The handset measures the arrival time of signals from three or more satellites, instead of antennas. The accuracy can vary from 2 meters in rural areas to 20 meters in urban areas.

Galileo satellite systems and GPS are well-known examples of Satellite Vehicles (SV)-Based Positioning Technology. Other examples are: EGNOS (European Geostationary Navigation Overlay Service), and Glonass (ex-USSR satellite-based localisation system). SV-based positioning techniques can be Mobile Terminated (MT) or Mobile Originated (MO). GPS is a technology funded by the US Department of Defense that uses transmitters on board of Satellite Vehicles and receivers held by the user. This technique is called Mobile Terminated (MT) and differs from Mobile Originated (MO) techniques, wich use transmitters on board of the user equipment. Information like positioning, speed and timing are only available to the receiver. In response to the US GPS system, the European Union and the European Space Agency started the Galileo satellite radio navigation system.[12] Satellite radio navigation is an advanced technology that can indicate the precise location or position of a moving or stationary object with an accuracy of one meter. Other than the GPS system, Galileo is not focused on defense applications, but on civil applications, like transport (navigation), social services (for disabled or elderly), justice (locaton of suspects), customs (border control), public works (GIS), search and rescue services (E112), and leisure (finding directions at sea or in the mountains).

Nonconventional Positioning Technologies are new positioning technologies that are becoming widespread. Examples of these new positioning technologies are Indoor

---

[11] See for example C Renso *et al*, 'Wireless Network Data Sources: Tracking and Synthesizing Trajectories', in T Gianotti and F Pedreschi (eds.), *see* note, p. 73-101; M Meints, D Royer, 'Location Information from a Technical Perspective', in C. Cuijpers, A Roosendaal, B-J Koops (eds), *D11.5: The legal framework for location-based services in Europe*. FIDIS Report D11.5, version 1.0, 12 June 2007, p. 15-24.

[12] European Commission, Directorate General Energy and Transport, *GALILEO*. On the Internet: *http://ec.europa.eu/dgs/energy_transport/galileo/index_en.htm*.

GPS, Bluetooth, and Wi-Fi. GPS positioning techniques sometimes have trouble i operating indoors because the signal strength is too low to penetrate the building. Indoor GPS uses a GPS-like navigation signal that is generated by a number of pseudosatellite devices. It can be used in wide space areas, like airport terminals and conference centers, where no significant barriers exist. Bluetooth is a tracking and positioning technique that makes it possible to locate a Bluetooth device (like a Bluetooth-enabled cell phone) and track the device's movement. The maximum range of a standard Bluetooth dongle is 100 meters. For indoor application, Bluetooth can have many advantages. Wi-Fi Positioning Systems (WPS) were originally developed for indoor purposes, but can also be used for outdoor purposes. WPS can replace GPS in urban areas, where the signal strength can be too low. By using Wi-Fi access points, the distance can be measured between at least three access points (trilateration) and the mobile device of the user with an accuracy up to 6 meters. WPS is very useful in urban and indoor areas, where there are enough access points.

There are also a number of other techniques with which location information can be generated: RFID, Biometrics, Machine Readable Travel Documents, Automated Teller Machines, and Optical Object Recognition.[13] An example of generating location information with RFID is the toll collection system. RFID can be used in road pricing systems. RFID systems can also use static RFID receivers in logistics, Tourist Information service points, electronic-detention systems etc. Biometric systems can generate location information by using static (optical) sensors such as video surveillance systems in combination with face recognition systems, finger printing systems, iris scan systems etc. Border control systems using ICAO-compatible Machine Readable Travel Documents (MRTDs), like passports, can also generate location information about the traveler. Automated Teller Machines and other paying machines where users identify themselves with a bank card can register where you are or where you have been. An example of generating your location with Optical Object Recognition is the license plate scanner.

These techniques can be categorised in the following table:

Category	***Technology***	***Method***
Cellular-Based Positioning Technologies	GSM; UMTS	Cell Identity; Cell Identity and Timing Advance; Enhanced Observed Time Differences; Assisted GPS

[13] See also M Meints, D Royer, 'Location Information from a Technical Perspective', in: C Cuijpers, A Roosendaal, B-J Koops (eds), *D11.5: The legal framework for location-based services in Europe*. FIDIS Report D11.5, version 1.0, 12 June 2007, p. 15-17.

Satellite Vehicles-Based Positioning Technologies	GPS; Galileo; Glonass; EGNOS	Mobile Terminated; Mobile Originated
Nonconventional Positioning Technologies	Indoor GPS; Bluetooth; WiFi; RFID; Biometrics; Machine Readable Travel Documents; Automated Teller Machines	Pseudosatellites; Trilateration; RFID receivers; Optical sensors; Optical object recognition

2.5 SMS Text Messages

Our GEOGOV research project covers a case study on the use of SMS Text Messages by the government. We are investigating a number of applications of SMS Text Messaging by the government: SMS Alert, Group SMS, SMS-Bomb and Cell Broadcast. SMS Alert is a service provided by the police to increase safety within a city district. Subscribers to an SMS Alert who live in a certain city district receive SMS Text Messages from the local police department for example when a child is missing, or when a burglar is active in the neighbourhood. A Group SMS is an SMS Text Message that is sent to a group of people who were in a certain area at a certain time, to ask them whether they have seen anything suspicious at a determined time and place. For example, an SMS Text Message was sent to 3000 people who were in the Nijmegen city centre at around 9 p.m. on the day a murder was committed. This system has been used in a number of murder cases in the Netherlands. An SMS Bomb is an SMS Text Message sent to discourage the use of a stolen cell phone. Every five minutes an SMS Text Message is sent to the cell phone that has been recorded stolen. Finally, governments can use Cell Broadcasts to send warnings by SMS Text Messages to people who are in a specific area. In fact, the message is sent to an area (a cell) instead of phone numbers. Every cell phone within this area can receive such a warning about an explosion, a flood, a toxic cloud, etc. Citizens only have to activate their cell phone to receive a Cell Broadcast message.

Some of these applications need personal data to perform. But even when no personal data is used, citizens may experience the receipt of such a message on their mobile equipment as an interference with their right to privacy, especially if they did not subscribe to the service.

3. Geo-Data Protection

3.1 Personal Data Protection

Privacy must be differentiated from *data protection*.[14] Data protection involves the 'traffic rules' for the protection of personal data, and is regulated at European level by the Directives 95/46/EC (Data Protection Directive), 2002/58/EC (Privacy and Electronic Communications Directive) and 2006/24/EC (Data Retention Directive). It is a rather two-fold or 'binary' decision to answer the question whether data protection legislation is applicable to LBS. The question is whether personal data is being processed or not. If so, the data protection legislation is applicable.

So, for the applicability of data protection legislation, it does not really matter whether someone experiences the processing of location data or geo-information about him as an interference with his privacy or private life. The processing of geo-information that is related to an identified or identifiable individual must comply with the above mentioned Directives, which must be implemented in national legislation and other applicable rules, like the ones in criminal procedure law. Because of the general international character of this contribution, we will focus on the above-mentioned data protection Directives, instead of on national regulations.

Directive 95/46/EC is applicable to "the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system" (Article 3, par. 1). For the applicability of the Directive it must be determined whether the information that is being processed is *personal data* in the meaning of Article 2 (a), and whether this personal data is being *processed* as meant in Article 2 (b).

3.2 Personal Data

3.2.1 Definition

'Personal data' is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." In Opinion 4/2007, the Article 29 Data Protection Working Party recently analysed the concept of personal data.[15] According to the Article 29 Working Party, there seems to be some uncertainty and some diversity in practice among the Member States with regard to the concept of personal data. The outcome of the analysis by the Article 29 Working Party would be especially relevant for topics like Identity Management in the context of eGovernment and eHealth, and in the RFID context.[16]

---

[14] See also C Cuijpers, 'A Private Law Approach to Privacy; Mandatory Law Obliged?' (2007) 4:4 *SCRIPTed* 304-318.

[15] Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*. Adopted on 20th June. 01248/07/EN, WP136.

[16] *Ibid*, at 3.

The definition of 'personal data' is very broad and includes all information concerning an identifiable individual.[17] This is confirmed by the Article 29 Working Party in their Opinion 4/2007.[18] Recital 26 of Directive 95/46/EC clarifies that "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person." The Directive is not applicable to the processing of personal data for purposes like public security, State security, defence, or criminal law, because these activities fall outside the scope of Community Law.[19] The data protection rules are also not applicable to the processing by a natural person for purely personal or household activities.

3.2.2 'Any information'

In their Opinion 4/2007, the Article 29 Working Party give explanations of the four 'building blocks' of personal data: 'any information', 'relating to', 'an identified or identifiable', 'natural person'. The explanation of 'any information' by the Article 29 Working Party shows that 'personal data' must be broadly interpreted. First, 'any information' can consist of objective information (the amount of glucose in one's blood) and subjective information (opinions, assessments). Subjective information can be used for the assessment of an individual at work or in society in general, and is therefore also considered 'personal data.' Second, information does not have to be correct or proven to be 'personal data': the data protection rules are also applicable to incorrect personal data. Third, 'any information' also means any sort of information, including sensitive data. Fourth, Directive 95/46/EC is applicable to personal data beyond the scope of the home and the family.[20] Activities of a professional or business nature are not excluded from the Directive.[21] Fifth, personal data is protected in any form: e.g. alphabetical, numerical, graphical, photographical or acoustic. It includes sound and image data relating to natural persons. Examples are the voice of a customer of a bank that has been recorded in telephone banking, an image captured by a video surveillance system, and a child's drawing that provides information about the child's mood and how it feels about different members of the family. Sixth, biometric data are personal data in two ways: it can be considered as content of information

---

[17] It must be noted that for example in the United Kingdom, this wide interpretation of 'personal data' has been narrowed by the English Court of Appeal in the case of *Durant v FSA* [2003] EWCA Civ 1746 *(http://www.bailii.org/ew/cases/EWCA/Civ/2003/1746.html).*

[18] *See* note 15, at 4.

[19] Directive 95/46/EC, Article 3. However, in 2005, the Commission published a *Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*. {SEC(2005) 1241}. Brussels, 4.10.2005. COM(2005) 475 final. 2005/0202 (CNS).

[20] European Court of Justice, 6 November 2003, Case C-101/01, (*Bodil Lindqvist v Sweden*) European Court reports 2003 Page I-12971: "The term undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies". The text of *Bodil Lindqvist v Sweden* is available on the Internet at *www.privacynetwork.info*.

[21] European Court of Human Rights, 23 November 1992 (*Niemietz v Germany*), series A No. 251/B; and European Court of Human Rights, 25 June 1997 (*Halford v The United Kingdom*), Reports 1997-III. The texts of *Niemietz v Germany* and *Halford v. The United Kingdom* are available on the Internet at *www.privacynetwork.info*.

about an individual (you have these fingerprints or DNA) and it can be considered as identifiers (this object has been touched by you).

3.2.3 'Relating To'

With regard to the second element, 'relating to', the Article 29 Working Party explains that information can be considered to *relate* to an individual, when the information is *about* that individual. It can be evident that information is related to an individual (e.g. the name, address, birth date of an individual), but it can also not be evident but only indirectly 'related to' an individual, like the value of your house. In 2005, the Article 29 Working Party explained when personal data is 'relating to' an individual: "data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated."[22] According to this explanation, a 'content' element, a 'purpose' element, or a 'result' element must be present.[23] When information is given 'about' a particular person, this information has a 'content' element. The result of a medical analysis is such information 'about' an individual. Information can also relate to an individual when the information is used or likely to be used with the 'purpose' to evaluate, treat in a certain way, or influence the status or behaviour of an individual. For example, the information on the use of a telephone inside a company office can be used for different purposes: to collect information about the use of the telephone by the employee, about the persons who were called, or about the cleaning staff that confirm by phone the time they leave. Finally, despite the absence of a 'content' or 'purpose' element, information can relate to an individual when the 'result' of using the information has an impact, minor or major, on the individual's rights and interests. An example is the monitoring of a taxi's positions by a taxi company using a satellite location system. The content is not related to a person but to a car and the purpose is not to evaluate the taxi driver's performance. However, this system can have an impact on the taxi drivers and therefore this data is subject to data protection rules.

3.2.4 'Identified or Identifiable'

The third element is that a person must be 'identified or identifiable.' This means that it should be possible to identify the person to whom the information is related to. Identification is possible by means of identifiers (height, hair colours, and clothing) or by a quality of the person (name, function, profession). A person can be identified directly (by name) or indirectly (by telephone number, passport number, etc.). A person can be identified indirectly when the information, combined with other information, makes it possible to distinguish the individual from others. Indirect identification is possible by factors like someone's physical, physiological, mental, economic, cultural or social identity. As a result, a person is for example identifiable by means of a device, like a personal computer or a cell phone, while it is possible to relate this device to its user. "All the means likely reasonably to be used" by the controller or by any other person to identify the individual should be taken into account to determine whether a person is identifiable. When these means are not

---

[22] Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology*. January 19, 2005. 10107/05/EN, WP105, p. 8.

[23] *See* note 15, at 10-12.

available, the individual is considered not to be identifiable and the information is not 'personal data'. A hypothetical possibility to identify the individual is not enough to consider a person to be identifiable. What should be taken into account are the costs of conducting identification, the intended purpose, the structure of the processing, the advantage expected by the controller, the interests of the individuals, risks like breaches of confidentiality, and technical failures. However, it should also be considered that identification may not be possible today, but could be possible when the information is still being processed in five years time. In this respect, the purpose of the data controller is also of importance for the identifiability of the data subject. For example, the purpose of a video surveillance system is to identify persons when necessary. This means that the whole video surveillance system must be considered as processing information about identifiable individuals. An IP address is also a personal data, because Internet service providers and managers of local area networks can identify Internet users by using reasonable means.[24]

3.2.5 'Natural Person'

The fourth element of 'personal data' is 'natural person', in other words human beings. This means that, with regard to the Directive, personal data is information related to an identified or identifiable *living* individual. Apart from a number of exceptions, the Directive is not applicable to the personal data of deceased persons. The exceptions are for example when the controller does not know that a data subject is no longer alive, or when data of a deceased person is related to a living individual at the same time,[25] or other sets of rules protect the personal data of a deceased individual, like medical secrecy, or when a Member State has extended the applicability of the national data protection rules to deceased persons.[26] Furthermore, whether the data protection rules are applicable to the personal data of unborn children depends on the general approach of the national legal system.

In principle, the Directive is not applicable to information about legal persons, although a small number of Member States have extended the application of their data protection law to legal persons.[27] Exceptions are to be found for example in Directive 2002/58/EC where subscribers, who can also be legal persons, are protected against unsolicited commercial communications. The question whether data protection law should also be applicable to legal persons is becoming relevant, because individuals' personal and professional lives are becoming more and more intertwined. Therefore,

---

[24] Furthermore, in Opinion 4/2007, the Article 29 Working Party also explains in this respect the meaning of pseudonymised data, key-coded data, and anonymous data (see note 15, p. 18-21).

[25] For example, personal data can be derived from personal data relating to the hereditary characteristics of one's parents. See also: R Gertz, 'An analysis of the Icelandic Supreme Court judgement on the Health Sector Database Act' (2004) 1:2 *SCRIPTed* 241-258.

[26] The fact that Directive 95/46/EC left unclear whether data protection rights are also applicable to deceased persons, resulted in a recommendation by the PRIVIREAL project to the European Commission to determine whether or not deceased persons should be included in the definition of a "natural person" in the Directive. European Commission Project, Privacy in Research Ethics & Law (PRIVIREAL). *(http://www.privireal.org/content/recommendations/#Recf).*

[27] D Korff, 'Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons' (2000) Commission of the European Communities (Study Contract ETD/97/B5-9500/78) Final Report, 02-02-2000. *(http://ec.europa.eu/justice_home/fsj/privacy/studies/legal-persons_en.htm).*

geo-information about an employee can be related to the individual but also to the organisation of the employer.

From the Opinion 4/2007 by the Article 29 Working Party, we can conclude that the definition of 'personal data' must be interpreted very broadly. This means that most information about a natural person must be considered to be 'personal data.' This is advisable for the protection of privacy of the individual, and for compliance with the data protection rules. It is obvious that geo-information falls within the scope of 'personal data' when the information relates to a natural person who can be identified. In that case, the general Directive 95/46/EC is applicable to geo-information. Because geo-information can be personal data and location data and/or traffic data at the same time, the special Directives 2002/58/EC and 2006/24/EC are also applicable to geo-information.

3.3 Electronic Communications Data

Electronic communications data is legally protected by national law, which implements Directive 2002/58/EC (Privacy and electronic communication, or e-privacy Directive).[28] More specifically, the Directive protects traffic data and location data. Both kinds of communication data are relevant in this context, because they can provide geo-information about where you are or where you have been.

The Directive defines traffic data as:[29]

> *any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.*

Traffic data refers, for example, to the routing, duration, time or volume of a communication. Traffic data that is used for mobile communications will also use location information about the terminal equipment (the mobile device) of the sender or recipient, to the network on which the communication originates and terminates, and to the beginning, end or duration of the connection.[30] These categories of information can be necessary for three kinds of purposes:[31] the transmission of the communication, the billing thereof, and the deliverance of value-added services.[32]

---

[28] 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 communications sector (Directive on privacy and electronic communications). *Official Journal* 2002, L 201/37, amended by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006. *Official Journal* 2006, L 105/54.

[29] Directive 2002/58/EC, Article 2(b).

[30] *Ibid*, Recital 15.

[31] See for example A Ekker, "Publiekrechtelijke bescherming van verkeersgegevens", in L Asscher and A Ekker (eds), *Verkeersgegevens, Een juridische en technische inventarisatie* (2003), available at *http://www.ivir.nl/publicaties/overig/gedeelteverkeersgegevens.pdf*

[32] A value-added service is "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." Directive 2002/58/EC, Article 2(g).

Value-added services may consist, for example, of advice on the least expensive tariff packages, route guidance, traffic information, weather forecasts, and tourist information. Value-added services are often location based services, because the information is often attuned to the actual location of the recipient.

The Directive defines location data as:[33]

> *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.*

Terminal equipment is for example a mobile phone or a pocket-pc (PDA). The geographic position is indicated by the latitude, longitude, and altitude of the terminal equipment.[34] Location data can also refer to the direction of travel, and the identification of the network cell in which the terminal equipment is located at a certain time.[35]

Location data can also be traffic data at the same time. For communications by mobile devices, information is being processed about the base transceiver station with which the mobile device is connected. This information is necessary for the transmission of the communication between the sender and the recipient. Location data is also traffic data at the same time, when location data is being used for the delivery of value added services.

Traffic data and location data are privacy-sensitive because they can be related to individual natural persons (users and subscribers). They can paint a picture of the user's communication behaviour, of his acting, and even of the content of his communications.[36] Traffic data can be data at the transporter and may not yet be related to an individual, they can provide information about the user's communication, necessary for the billing,[37] or even about the content of the communication.[38] Location data is more precise than is necessary for the transmission of communications. With location data it is also possible to follow the user or subscriber 'in real time'. Therefore, location data can be even more privacy-sensitive than traffic data. That is why, according to Directive 2002/58/EC, the processing of location data is only allowed when subscribers have given their consent.[39]

According to Directive 2002/58/EC, the processing of location data is only allowed:

- when they are made anonymous; or

---

[33] Directive 2002/58/EC, Article 2(c).

[34] Positioning techniques used for locating the terminal equipment can for example be cellular based (GSM) or satellite based (GPS). See also s. 2.4.

[35] Directive 2002/58/EC, Recital 14.

[36] *See* note 31, at 47.

[37] For example, Alice called Bob at 3.00 p.m. from the Princes Street Gardens in Edinburgh, while Bob was at the Edinburgh University and moving to the Castle.

[38] For example, Alice downloaded the programme of a political party and ordered a folder by which she can subscribe as a member of that political party.

[39] Directive 2002/58/EC, Recital 35.

- with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.[40]

Furthermore:

- When the subscribers or the users have been informed by the service provider prior to obtaining their consent about:
  - the type of location data other than traffic data which will be processed;
  - the purposes of the processing;
  - the duration of the processing; and
  - whether the data will be transmitted to a third party for the purpose of providing the value added service;
- when the processing of location data is necessary for the purposes of providing the value added service.
- When the service provider gives the users or subscribers 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.
- When the processing of location data is restricted to persons 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 is restricted to what is necessary for the purposes of providing the value added service.

Subscribers and users have the right to withdraw their consent for the processing of location data at any time. After users or subscribers have given their consent, the processing of location data (being traffic data) is only allowed when and as long as it is necessary for delivering the value added service. After that, the location data can only be used for billing purposes. As soon as the bill has been paid, and the bill is not disputed, the location data has to be deleted or anonymised.

One of the conditions for processing location data, mentioned above, is that the service provider should inform the users or subscribers about the possibility of temporarily refusing to grant permission to process their data, using simple, free means. However, it is possible that within Member States the service providers can override the elimination of calling line identification in instances of malicious or nuisance calls, or in case of emergency calls, for the purpose of responding to such calls.[41]

Member States can limit the scope of the rights and obligations with regard to traffic data and location data (Article 15). This is possible when such a restriction is a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences. In such a case, a service provider is allowed to comply with a request to provide location data to a law enforcement agency.

---

[40] *Ibid*, Article 9.1.

[41] *Ibid*, Article 10.

Location data that is not anonymised is also personal data. Therefore, Directive 95/46/EC is also applicable to the processing thereof. This means for example that the data subject has a right of access to his own personal data[42] and that the processing of the location data must be in compliance with the criteria for making data processing legitimate.[43] An employer (subscriber), who has subscribed to a geo-location service, must verify whether the service provider (operator) acts in compliance with the rules for electronic communications. Otherwise, the employer might process and use the location data in an illegitimate way.[44]

Location data about employees may be processed only by the network operator, the provider of the value-added service, and by the employer. These actors can process the same location data, but they might use that data for different purposes. The network operator processes location data to establish the communication. The operator concludes a contract with the employer (subscriber), who, in turn, puts the terminal equipment at the disposal of the employee (user). The location data can then be used for locating the employee. The same operator or the service provider can offer the value-added service by using the location data about the employee that has been provided by the operator. The employer can receive the same data from the operator to be able to monitor the employee. As a result, the operator can provide the location data to the employer, if necessary through the service provider. Such transmissions fall under the scope of the processing of personal data, as meant in the Directives 95/46/EC and 2002/58/EC, and are only allowed when they comply with their provisions. [45]

3.4 Data Retention

At the end of April 2004, shortly after the Madrid attacks, the United Kingdom, France, Ireland and Sweden proposed to the Council of the European Union to introduce a general retention period of 12-36 months for electronic communications traffic data for the prevention, investigation, detection, and prosecution of criminal offences. This would result in the systematic retention of traffic data about telephone conversations, including cell phone communications, e-mail communications and web pages visited on the Internet, of about 450 million European citizens. The proposal has resulted in Directive 2006/24/EC.[46] This Directive amended Article 15 of Directive 2002/58/EC by inserting a new paragraph 1a, that should bring an end to the variety of data retention periods in the Member States. Therefore, the aim of Directive 2006/24/EC is the harmonization of data retention laws. The Directive applies to traffic data and to location data, but not to the content of electronic communications. However, sometimes it is quite easy to deduce content information from traffic data or location data, like from the websites you have visited.

---

[42] Directive 95/46/EC, Article 15.

[43] *Ibid*, Article 7.

[44] D de Bot, S Renette, "Employee, where are thou?" (2006) *Privacy & Informatie* 210-214.

[45] *See* note 44, 214.

[46] 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* 2006, L 105/54.

Article 5 of Directive 2006/24/EC gives an overview of the categories of data that have to be retained by the providers of public electronic communication services:

- data necessary to trace and identify the source of a communication;
- data necessary to identify the destination of a communication;
- data necessary to identify the date, time and duration of a communication;
- data necessary to identify the type of communication;
- data necessary to identify users' communication equipment or what purports to be their equipment; and
- data necessary to identify the location of mobile communication equipment.

The data that is necessary to trace and identify the source of the communication, concerning fixed network telephone and mobile telephony are the calling telephone number and the name and address of the subscriber or the registered user. Concerning Internet access, Internet e-mail, and Internet telephony, these data are the user ID(s) allocated, the user ID and telephone number allocated to any communication entering the public telephone network, and the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication. The data that is necessary to identify the location of mobile communication equipment is the location label (Cell ID) at the start of the communication, and data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data is retained.

The Member States must ensure that all this data is being retained by providers of electronic communications for a period of not less than six months and not more than two years from the date of the communication.[47] The European Parliament and the Council are of the opinion that the retention of this data is a necessary and effective investigative tool for law enforcement in several Member States, with regard to Article 8 ECHR:[48]

> *9. […] Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society, inter alia, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organized crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. The adoption of an instrument on data retention that complies with the requirements of Article 8 of the ECHR is therefore a necessary measure.*

---

[47] Directive 2006/24/EC, Article 6.

[48] *Ibid*, Recital 9.

In the explanatory memorandum to the Data Retention Bill, the Dutch government cited a research report by the Erasmus University Rotterdam about the benefit and necessity of the obligation to retain historical traffic data about electronic communications.[49] The report concluded that a retention period of three months could be sufficient for simple criminal investigations at district level. However, such a period would be too short for long term and complex investigations at regional and national level. Examples are: investigations of drug crimes, serious environment crimes, trafficking in human beings, organised fraud, murder, and serious sexual offences. Legal requests for assistance and investigations of cold cases are also examples that would need a longer retention period, according to this research.

On 11 March 2008, the German Supreme Court (*Bundesverfassungsgericht*) limited the scope of the German Data Retention Act.[50] The Court concluded that the traffic and location data can only be claimed and used by law enforcement agencies in investigations of serious crimes. It is forbidden to claim and use this data for pattern analysis with electronic communications data and for investigating crimes committed by electronic communications.

In the parliamentary discussions in the Netherlands, senator Hans Franken who is also a professor in IT and Law at Leiden University, characterised the Dutch Bill which is used to implement Directive 2006/24/EC into Dutch national legislation, as 'nonsensical', 'dangerous', and 'involving considerable expenses'.[51] According to Franken, it is nonsensical because as a result of the large amount of traffic data and location data that will be retained. Law enforcement agencies will be searching for a needle in a haystack. It is also dangerous, because this large amount of data will probably be stored at a central institute, which would make its access vulnerable to criminals. Finally, it is foreseeable that the communication providers will pass on the additional expenses to the consumer. As a result, the retention of traffic data and location data is not only a threat to the consumer's privacy, but also to his bank account. Would consumers value their privacy more if they realised what the financial consequences of the retention of their geo-data were?[52]

---

[49] *Kamerstukken II*, 2006/07, 31 145, n 3, p 5. The report is available (in Dutch) at: *http://www.justitie.nl/images/aanbieding%20rapport%20Erasmus%20Universiteit_4147_tcm34-14299.pdf*

[50] Bundesverfassungsgericht, "Eilantrag in Sachen 'Vorratsdatenspeicherung' teilweise erfolgreich", Press Report Nr. 37/2008, 19 March 2008. *(http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg08-037)*

[51] A Veenman, "Senator Franken ten strijde tegen dataretentie wetsvoorstel", *(http://www.ispam.nl/archives/591/senator-franken-ten-strijde-tegen-dataretentie-wetsvoorstel)*

[52] On 22 May 2008, the proposed retention period in the Bill has been amended by the Dutch House of Representatives and decreased from 18 months to 12 months. *Handelingen* 2007/08, n 87, Tweede Kamer, 6155-6156.

4. Reasonable Expectations of Privacy in Public Places

4.1 Privacy According to Citizens

What people experience as an interference with their privacy or private life is being regularly surveyed.[53] In 1999, the Dutch national technology assessment organisation (Rathenau Institute) published the results of a privacy survey.[54] The survey shows that Dutch citizens associated the following nine values with the concept of privacy: (1) independence, (2) freedom of movement, (3) equality, (4) freedom from stigmatization, (5) undisturbed life, (6) self-esteem, (7) freedom from manipulation, (8) integrity, and (9) autonomy.

Recently, the Dutch National Freedom Survey 2007 (Nationaal Vrijheidsonderzoek 2007) shows that between 2002 and 2007, the importance of privacy was constantly valued.[55] Throughout these years, about 39% of the Dutch citizens considered the right to privacy as the most important fundamental right. This survey also shows how citizens experience security measures in relation to an interference with their right to privacy.

Citizens think that the following measures are a relatively small interference with privacy:

- camera surveillance in public places; and
- the obligatory identification for every citizen of 12 years or older.

The following measures are considered to be a relatively more serious interference with a person's privacy (in ascending order):

- the transfer of passenger data by airline companies to the country of destination;
- tracing and recording people's location by automatic scanning and of car license plates;
- the government taking everyone's DNA-profile;
- preventive searches by the government;
- tracing and recording people's location through mobile phone traffic data;
- preventive custody of a suspect;
- a house search on the grounds of suspicion;
- government monitoring of every e-mail and Internet communication; and
- government eavesdropping of every telephone communication.

Nowadays, the youth show a more selective opinion regarding their privacy. However, another recent survey by Digibewust and Mijn Kind Online (November

---

[53] See for example Roger Clarke's Survey List: *Reference List: Surveys of Privacy Attitudes*, available on the Internet: *(http://www.anu.edu.au/people/Roger.Clarke/DV/Surveys.html)* (started in 1996 with revisions to 2006); EPIC Public Opinion and Privacy Page, available at *http://epic.org/privacy/survey/.*

[54] G Smink, A Hamstra, H van Dijk, "Privacybeleving van burgers in de informatiemaatschappi" (1999) *Werkdocument* 68, 11.

[55] D Verhue, *Nationaal Vrijheidsonderzoek* – opiniedeel meting 2007, Amsterdam: Veldkamp, April 2007.

2007) shows that young people (12-18 years old) willing leave their pictures and their names on social networking sites on the Internet.[56] Despite this, they do seem to be a lot more careful with their phone numbers and addresses. The British Information Commissioner's Office (ICO) web page 'Social networking' also warns young people in particular that their privacy, their professional career, or even their personal safety is at risk when putting personal information online on social networks. In November 2007, the ICO published a leaflet entitled: "Using social networking sites safely to stimulate privacy awareness and encourage the safe use of social network sites by young people."[57]

4.2 Reasonable Expectations of Privacy

The question whether the right to privacy has been invaded is more difficult to answer than the question whether data protection rules are applicable. This is mainly because privacy is a rather vague concept, and difficult to define. Warren and Brandeis' well-known definition is 'the right to be left alone'.[58] This definition, and more generally the whole concept of privacy, illustrates that privacy is a rather 'personal' thing. Not just because the function of privacy is to protect individuals, but also because every individual may have their own opinions about what he or she experiences as an unwanted interference with his or her privacy. From the aforementioned Dutch National Freedom Survey 2007, it appears that 63% of the respondents (Dutch citizens) think that locating people by cell phones is a major interference with their private life. At the same time, 37% of the respondents think that this is not a major interference with their private life. Therefore, other than the 'binary' decision whether data protection legislation is applicable, the decision to decide whether privacy is invaded is not so easy to make and appears to be an individual balancing of interests.

However, there is a concept that could make it possible to give an objective answer to the question whether there is an interference with the privacy of an individual. This concept is the *reasonable expectations of privacy* test. This litmus test was introduced in 1967 in the United States by Judge John Marshall Harlan in his concurring opinion in the US Supreme Court case of *Katz v United States*.[59] In this case, a telephone call by Katz, made from a glass phone booth, was overheard and recorded by FBI agents. The Supreme Court concluded that an enclosed telephone booth is an area where, like a home, a person has a constitutionally protected reasonable expectation of privacy. Furthermore, the Supreme Court concluded that electronic as well as physical intrusion into a place that is in this sense private, may constitute a violation of the Fourth Amendment. Finally, the Court concluded that the invasion of a constitutionally protected area by federal authorities is, as the Court has long held, presumptively unreasonable in the absence of a search warrant. The Supreme Court

---

[56] "Nemen van privacyrisico's inherent aan opgroeien" *Webwereld*, 27 November 2007.

[57] Information Commissioner's Office, "Using social networking sites safely", *(http://www.ico.gov.uk/Home/for_the_public/topic_specific_guides/social_networking.aspx)*

[58] S Warren and L Brandeis, "The Right to Privacy" (1890) 4 *Harvard Law Review* 193.

[59] 389 U.S. 347 (1967). See also R Gellman, "A General Survey of Video Surveillance Law in the United States" in S Nouwt, B de Vries, C Prins (eds), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy* (2005) The text of *Katz v United States* is available at *www.privacynetwork.info*.

stated that "the Fourth Amendment protects people, not places." For Mr. Justice Harlan, this raised the question what protection it affords to those people. According to Harlan, the answer to that question requires reference to a 'place'. This resulted in the *reasonable expectations of privacy* test. According to this test, there are two standards to determine whether a person can have a reasonable expectation of privacy. First, a person must have an actual (subjective) expectation of privacy in a certain situation. Second, society is prepared to recognise this (objective) expectation as reasonable. As a result, a man's home is a place where he expects privacy. In this case, Katz expected that his telephone conversation would not be intercepted after closing the door of the telephone booth and paying the toll to place a call.

The *reasonable expectation of privacy* test has also been recognised in several judgments from the European Court of Human Rights (ECtHR). In the case of *Lüdi v Switzerland*, the ECtHR concluded that a citizen who is involved in criminal activities (drug trafficking) has a less expectation of privacy.[60] In this case, the undercover police officer installed technical devices in order to gain access to Lüdi's home and record his conversations. The Court concluded that Lüdi must have been aware that he was engaged in a criminal act and that he was running the risk of his private life being interfered with by an undercover police officer.

In the case of *Halford v the United Kingdom*, the ECtHR used the *reasonable expectations of privacy* test for the first time.[61] The Court recognised that having a telephone conversation at the workplace falls within the scope of 'private life' and 'correspondence' of Article 8 ECHR. In this case, the Court concluded that it had not been proven that Mrs. Halford had been warned by her employer (the Merseyside police headquarters) that her telephone conversations could be monitored. As a result, she would have had "a reasonable expectation of privacy for such calls", according to the Court.

However, for the protection of privacy the *reasonable expectations of privacy* test is not without risks. In this respect, Paul Schwartz has indicated the risk of the 'silent ability of technology to erode our expectations of privacy', pointing to the principal theme of the struggle about defining expectations of privacy in relation to new technologies.[62] We could say that the *reasonable expectation of privacy* is diminishing as a result of the ongoing technological possibilities for monitoring citizens. If this is true, then we are sitting on a sliding scale of privacy: the more personal information becomes public, the less privacy we have. However, any interference with our private life, including monitoring citizens, is limited by the conditions of the second paragraph of Article 8 ECHR, which states that an interference with our 'private and family life, home and correspondence' is only allowed in the following cases:

- in accordance with the law and
- necessary in a democratic society in the interests of:

---

[60] European Court of Human Rights, Judgment of 15 June 1992 (*Lüdi v Switzerland)*, Publ. ECtHR, Series A, No. 238. The text of *Ludwig Lüdi v Switzerland* is available at *www.privacynetwork.info.*

[61] European Court of Human Rights, Judgment of 25 June 1997 (*Halford v The United Kingdom*), no. 200605/92, 1997.

[62] Paul Schwartz, "Privacy and Participation: Personal Information and Public Sector Regulation in the United States" (1995) 80 *Iowa Law Review* 553, 573, cited in Robert Gellman, note 59.

- 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.[63]

The condition of 'necessity' means that there must be a 'pressing social need' to make an interference. A pressing social need means that there must be 'need-to-know' personal information; that it would be 'nice-to-know' is not sufficient. Necessary also means that the purpose cannot be achieved without the interference (proportionality principle), and that the purpose cannot be achieved by less privacy invading measures (subsidiarity principle). In 2006, the Dutch Attorney General Brouwer suggested, with regard to the collection of road pricing traffic data, that "those traffic data can be very useful for criminal investigations." This is a typical example of 'nice-to-know', and therefore it seems very questionable whether this would be a lawful interference with the privacy of the motorists. That road pricing could also be realised without logging the 'trajectories' of the motorists by GPS, has been argued by the Dutch entrepreneur professor Roel Pieper. As early as 2001, he introduced the idea of creating a system of road types. The idea is to divide the road system into a limited number of road types and to base the calculation of the price on the use of the number and kind of road types. This is an example of applying the subsidiarity principle.

With regard to the government's use of citizens' geo-information, an important question is whether citizens have a reasonable expectation of privacy in public places? The answer seems to be affirmative, as will be illustrated later.

4.3 Privacy in Public Places

4.3.1 Definition of 'Public Place'

What actually distinguishes a private place from a public place seems obvious, but this led in 2004, at least in the Netherlands, to discussions in parliament when the Bill on Camera Surveillance in Public Places was discussed.[64] The (present) Act is only applicable to camera surveillance for the prevention of public disorder in municipalities. The explanatory memorandum defines 'public place' as "a place that is open to the public, according to its function or regular use". 'Open to the public' means that there are no barriers to enter the place, like a duty to report, preceding permission, or levying an admission ticket. As a result, stadiums, post offices, department stores, restaurants, and hospitals are in this respect not considered as public places.

'Function' refers to the nature given to the place. The nature of a place may follow from a decree or from the purpose that follows from the functionality of the place.

---

[63] According to the European Court of Human Rights, Article 8(2) ECHR has to be interpreted narrowly. *See* European Court of Human Rights, Judgment of 4 May 2000 (*Rotaru v Romania*), no. 28341/95, § 47.

[64] 'Wet tot Wijziging van de Gemeentewet en de Wet politieregisters in verband met de invoering van regels omtrent het gebruik van camera's ten behoeve van toezicht op openbare plaatsen' (*camera surveillance in public places*). *Kamerstukken II*, 2004/05, 29 440.

A place becomes a public place through 'regular use' when this is used for this purpose, and the rightful claimant allows the place being used as such. Therefore, a public place is a place where people come and go, like for example:

- the street,
- the (public) road and in the continuation thereof:
- public gardens,
- playing fields,
- parks,
- open sections of indoor shopping centers and arcades.

Shops, discotheques, parking garages, town halls, churches and mosques, public sections of a railway stations (if private property) are private, not public places.

During the discussion of the Dutch Camera Surveillance Bill, the Christian Democratic Party stated that in their opinion it is impossible to have a right to privacy in a public place because whoever exposes themselves in a public place would relinquish the right to see this as a private part of their lives. Therefore, there is no question of interference of an individual's private life in a public place.[65]

As we will show hereafter, this opinion obviously differs from that of the European Court of Human Rights (ECtHR),[66] but also from the opinion of the Dutch government. According to the Dutch government, the right to privacy is not spatially limited. The government refers to a judgment by the Dutch Supreme Court in 1991, about the seizure of videotapes from a public demonstration,[67] and concludes that camera surveillance on a public road can interfere with the right to one's private life. However, according to the Dutch government, the more public a citizen's behavior is, the less the right to privacy will be an issue. So, according to the Dutch government, a citizen's behavior can be less or more public. This also means that a citizen can expect less or more privacy.

The right to privacy protects our 'private and family life, home, and correspondence' (Article 8 ECHR). These four elements are typical elements of our privacy. Therefore, it seems that the right to privacy is especially applicable to private places. However, at present these private places do not seem to be so private anymore: we store a lot of our personal data on our personal hard disks, laptops, Blackberries, or iPods; a lot of personal information is stored on the servers of our Internet service provider or on Google's servers; our personal computers are easy victims for computer searches by law enforcement agencies because physical admittance is no longer necessary; all our telephone and electronic communications data is being retained by service providers to be made available when needed for law enforcement, etc. Big Brother is not only watching you, but he also knows where you are, where you have been and probably even where you are going to. Thanks to the technical possibilities for large scale collection and analysis of personal data, including geo-information (location data,

---

[65] *Kamerstukken II*, 2004/05, 29 440, n 6, p 10.

[66] See particularly European Court of Human Rights, Judgment of 25 September 2001 (*PG and JH v The United Kingdom*), no. 44787/98. The text of *PG and JH v The United Kingdom* is available on at *www.privacynetwork.info.*

[67] Dutch Supreme Court (Hoge Raad) 19 February 1991, *NJ* 1992, 50.

whereabouts), telecommunications data, etc., it will become much easier, for example, for law enforcement agencies to compare this data with so called risk profiles. As a result, the privacy of ordinary citizens will come under pressure because they are becoming more transparent to law enforcement and intelligence agencies. It also enhances the risk of mistakes being made because criminal investigations could then be extended to cover everyone. There is a big difference between legitimising the preventive monitoring of everyone and the limited application of a means of coercion against specific suspects.[68]

If we do not have privacy any longer in our private places, do we have privacy then in public places? Or are there any private places in public space? This question is of special importance for the collection, storage, and use of geo-information about citizens. In the following section, we will analyse how the European Court of Human Rights (ECtHR) has recognised the right to privacy in public places.

4.3.2 European case law

In 2000, the European Court of Human Rights (ECtHR) passed a judgment on the difference between private and public places in the case of *Rotaru v Romania*.[69] In this case, the ECtHR confirmed their earlier judgments by recognising that information about the applicant's life, in particular his studies, his political activities and his criminal record, when systematically collected and stored in a file held by agents of the State, falls within the scope of 'private life' for the purposes of Article 8 ECHR.[70] The Court disagreed with the Romanian government that this information is related to the applicant's public life, and therefore did not fall within the scope of 'private life'. With regard to public information that can fall within the scope of the right to private life, the Court made an interesting remark:

> *Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past.*[71]

The Court recognised that a right to privacy exists when a government agency systematically collects and stores personal information, even when this is public information.

In the case of *P.G. and J.H. v The United Kingdom,*[72] the Court dealt with the scope of privacy in public places. The applicants complained that covert listening devices were used by the police to monitor and record their conversations in an apartment, that information was obtained by the police concerning the use of a telephone at the

---

[68] About trends in intelligence and security measures and privacy risks, see also: A Vedder, *et al*, *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw* (2007) (with English summary), available at *http://www.rathenau.nl/showpageBreed.asp?steID=1&ID=3814*

[69] European Court of Human Rights, Judgment of 4 May 2000 (*Rotaru v Romania*), no. 28341/95.

[70] *Ibid*, § 44.

[71] *Ibid*, § 43.

[72] European Court of Human Rights, Judgment of 25 September 2001 (*PG and JH v The United Kingdom*), no. 44787/98.

apartment, and that, while they were at the police station, listening devices were used to obtain voice samples. In the Court's opinion, there is an area, also in public space, where people may have interactions, which are protected by the right to privacy:

> *There is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life.'*[73]

Furthermore, the Court gave a number of elements that are relevant to the consideration of whether a person's private life is concerned by measures effected in public places:

> *Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method…*[74]

The Court concluded that the recording of the voices of the suspects at the police station was an interference with their right to respect for private life. In this case, the Court recognised that personal information collected in a public place, falls under the scope of the right to privacy when this information has been collected and stored systematically, for example by a government agency. This conclusion can also be applied to geo-information, when that information is related to an identified or identifiable natural person. Systematically collecting, storing, and analysing geo-information must be considered an interference with the right to privacy of the individual. The next question is whether the interference is legitimate.

In August 1995, a British citizen (Peck) walked down Brentwood High Street (UK), carrying a kitchen knife in his hand and attempted suicide by cutting his wrists.[75] Unknowingly, his action had been filmed by a CCTV camera. Although the footage did not show Peck actually cutting his wrists, the operator was alerted because of the possession of a knife. The police were notified and having arrived at the scene, took the knife, gave the applicant medical assistance, and after bringing him to the police station released him without charges. In October 1995, photographs taken from the CCTV footage, with Peck's face unmasked, were published in a number of

---

[73] *Ibid*, § 56.

[74] *Ibid*, § 57.

[75] European Court of Human Rights, Judgment of 28 January 2003 (*Peck v The United Kingdom*), no. 44647/98, available at *www.privacynetwork.info*.

newspapers. In the meantime, the Brentwood Borough Council also disseminated the footage for a documentary program to Anglia Television and to the BBC producers of 'Crime Beat'. Afterwards, Peck was recognised in the newspapers and on television by family and friends. Peck complained to the Court that the Brentwood Council disproportionately interfered with his right to private life by the disclosure of the CCTV footage. The Court agreed with Peck that a serious interference with his private life had been made because the pictures of the relevant moment were viewed to an extent which far exceeded any exposure to a passer-by or to security observation, and to a degree surpassing that which Peck could possibly have foreseen when he walked in Brentwood High Street on that day.

In the case of *Peck v The United Kingdom*, the Court also refers to two other judgments by the European Commission of Human Rights (the Commission) about collecting photographs of people in public places and the unforeseeable use thereof. In the case of *Friedl v Austria*, the Commission concluded that there was no intrusion with Friedl's right to privacy because the photographs were taken of a public demonstration related to a public event and that they had only been used as an aid to policing the demonstration.[76] Furthermore, the photographs remained anonymous.

In the case of *Lupker and Others v The Netherlands,* the Commission concluded that the police only used photographs to identify offenders in criminal proceedings, and that there was no reason to believe that the photographs have been made available to the general public or that they would be used for any other purpose.[77]

The case of *Perry v The United Kingdom*[78] deals with the right to privacy in the public place of a police station. Mr. Perry agreed to participate in an identification parade on 5th of June 1997, with regard to a series of armed robberies, but in the end, he did not show up. Because he neither appeared in a number of other identification parades, the police decided to video him with the custody suite camera of the Bilston Street police station. A compilation tape was made and shown to a number of witnesses of the armed robberies of whom two positively identified him as involved in one of the robberies.

With reference to the case of *P.G. and J.H. v The United Kingdom*, the court concluded in *Perry v The United Kingdom* that the right to privacy can also exist outside a person's home or private premises.[79] In the case of *Perry v The United Kingdom*, the applicant did not expect that video footage would be taken of him within the police station for use in a video identification procedure and, potentially, as evidence prejudicial to his defence at trial. The recordings went beyond the normal and expected use of this type of camera, what is demonstrated by the fact that the police had to obtain permission and an engineer had to adjust the camera.

---

[76] *Friedl v Austria*, judgment of 31 January 1995, Series A no. 305-B, Friendly Settlement, Commission report of 19 May 1994.

[77] *Lupker and Others v The Netherlands*, no. 18395/91, Commission decision of 7 December 1992, unreported.

[78] European Court of Human Rights, Judgment of 17 July 2003 (*Perry v The United Kingdom*), no. 63673/00, available at *www.privacynetwork.info*.

[79] *Ibid*, § 37.

The Court considered that the recording and use of the video footage of the applicant in this case discloses an interference with his right to respect for private life. Furthermore, the Court concluded that this interference is not in accordance with the (British) law, because the police failed to comply with the Police and Criminal Evidence Act 1984 and with the Code of Practice annexed to this Act, which concerned the failure to ask the applicant for his consent to the video, to inform him of its creation and use in an identification parade, and of his own rights in that respect.[80]

In *Perry v The United Kingdom,* the Court also concluded that camera surveillance in public places without recording the visual data, does not as such result in an interference with the individual's private life.[81] Also the normal use of security cameras whether in the public street or on premises, where they serve a legitimate and foreseeable purpose, does not interfere with the right to private life.[82] However, this situation is changing as a result of the new technological developments for recording personal data and by the systematic and permanent character of the files in which this data is stored. The publication of the recorded data that is not normally foreseeable, may also bring such security recordings within the scope of Article 8 ECHR. That was also the opinion of the Court in the case of *Peck v The United Kingdom*, when the disclosure of the video footage to the media for broadcasting on television, was considered a serious interference with the applicant's private life, notwithstanding that he was in a public place at the time.[83]

Despite the fact that celebrities are public figures, they also have a right to respect for their private lives. An example is the case of Princess Caroline von Hannover, daughter of Prince Rainier III of Monaco. Photographs of Caroline von Hannover were taken in private situations (not in her function as a Princess) and published in the German tabloid press.[84] According to the Court, the determining factor that allows the publication of pictures of public figures is the contribution they can have to a debate of general interest. In the case of Caroline von Hannover, there was no contribution to such a debate, because the pictures were not made of her in an official function but were related to details of her private life only. That is why in this case the right to privacy overrules the freedom of expression. Furthermore, the Court considered that each individual, including public figures like Caroline von Hannover, should have "*a legitimate expectation of protection of her private life*."

5. Conclusion

Modern positioning techniques make time and place relevant issues again. They make it possible to locate mobile terminal equipments and their users. As a result, like the private sector, governments are able to deliver a new kind of services: Location Based Services (LBS), based on the use of geo-information.

---

[80] *Ibid*, § 47.

[81] *Ibid*, § 38.

[82] *Ibid*, § 40.

[83] *Ibid*, § 38.

[84] European Court of Human Rights, Judgment of 24 June 2004 (*Von Hannover v Germany*), no. 59320/00.

It is obvious that the use of postioning techniques, described in section 2, also makes it interesting to collect geo-information for profiling purposes. Geo-information, combined with other types of personal data, can provide new possibilities for finding patterns, sequences, and relationships e.g. in the fields of marketing, crime control, or insurance. From a privacy perspective not only the application of data protection regulation is relevant, but also more fundamental interests, like autonomy, democracy, pluralism, non-discrimination, rule of law and balanced control.[85]

Governments that (are preparing to) offer LBS, should be aware of the data protection rules and the privacy expectations of the citizens. With regard to the data protection rules, we are of the impression that up to now, governments have been paying too scant attention to the application of these 'traffic rules' to protect personal data. With regard to the applicability of these data protection rules, there is one important rule of thumb: data protection rules are applicable when personal data is being processed. It leads to a rather binary conclusion: applicable or not.

On the other hand, as regards the extent citizens expect privacy when geo-information, and more particular LBS is used, appears to be more complicated. We have discussed two concepts that might provide guidance to answer this question in specific cases. The first one is the *reasonable expectations of privacy* concept, introduced by Judge John Marshall Harlan, former member of the American Supreme Court in 1967, and also accepted in a number of judgments by the European Court of Human Rights. This concept means that a right to privacy should be recognised if 1) a person has exhibited an actual (subjective) expectation of privacy, and 2) that expectation is one that society is prepared to recognise as reasonable. The second concept is Article 8 of the European Convention for the Protection of Human Rights, more specifically paragraph 2, requiring compliance with the necessity principle, including proportionality and subsidiarity.

The European Court of Human Rights has recognised the existence of the right to privacy in public places. Therefore, while geo-information about citizens will in general be collected in public places, governments should also realise that citizens can have legitimate privacy expectations with regard to the use of geo-information. However, the distinction between a private and public place is diminishing. This is illustrated by the fact that even in a public space there are private places, and by the fact that new technologies make it easier to have access to the citizens' personal information, because this information is more often stored on mobile devices and on servers from service providers who are obliged to retain those data for a certain period, especially for law enforcement purposes. As a result, the distinction between public and private seems to fail as a litmus, but the *reasonable expectation of privacy* concept could still be a standard for the law to rely on.[86] And within the context of geo-information, this standard might work even better because privacy protects people and not places.

However, we can also conclude that the *reasonable expectation of privacy* concept appears to be already diminishing as a result of the ongoing technological possibilities of locating and monitoring citizens. The result could be that citizens may no longer

---

[85] About profiling, *see* L Bygrave, *Data Protection Law. Approaching Its Rationale, Logic and Limits* (2002), especially Part IV: Profiling – Regulation by Data Protection Laws.

[86] *See* note 59, 35.

have actual expectations of privacy (the subjective element), or that society might no longer recognise these expectations as reasonable (the objective element) because the technology has become of common use. In that case, we are on a sliding scale of privacy: the more personal information is public, the less privacy we have. Fortunately, we still have our second privacy concept: Article 8 ECHR, especially paragraph 2. The necessity principle, including the proportionality and subsidiarity principle, seems to provide a better guidance for determining whether an interference with our private life is legitimate. There must be a 'need-to-know' factor about citizens' personal data and the purpose for collecting personal data could not be realised with other means that are less invasive of privacy. In this era of technological turbulence, these principles seem to provide a better basis than the *reasonable expectations of privacy* concept. However, the recognition by the European Court of Human Rights might also be considered an uncertain factor because it does not require blood, but technology, to violate the right to privacy.[87] It will be clear that questions like these remain to be discussed, and hopefully this article will stimulate those discussions.

[87] P de Hert, "Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11" (2005) 1 *Utrecht Law Review* 89.
(http://www.utrechtlawreview.org/publish/articles/000005/article.pdf)