Power and privacy

van Ooijen, C.W.; Nouwt, J.

Published in:
SDI Convergence

Publication date:
2009

Document Version
Peer reviewed version

Power and Privacy: the Use of LBS in Dutch Public Administration

Charlotte van Ooijen and Sjaak Nouwt[1]

Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, the Netherlands, C.W.vanOoijen@uvt.nl

Abstract
There are in the policy fields of traffic management as well as public order and safety in the Netherlands new applications of location-based services (LBS) such as the public transport chip card and the use of mobile phone location data in policing. Combining citizens' location information and personal data is essential for the provision of LBS. We explored three cases of LBS in Dutch public administration and argue that LBS may affect the balance between the roles citizens can have in their relationship with government: subject, client and citoyen. Consequently, we discuss the concept of privacy in public places and relate this to European case law. It is important for government to be aware of the powerful inherent logic of LBS and how this may shape government-citizen interaction.

Keywords: Location-based Services (LBS), public administration, citizenship, privacy.

1. INTRODUCTION

"As Dutch citizens we are well taken care of by our state. Just look at our beautiful road infrastructure. Even the tiniest village in the outskirts of the country can be easily reached. Diverse access ways have been constructed into our big cities. As clients of our government we are entitled to use this well-maintained system, at a fair price of course, which is determined by our road tax system. And now the very good news is that a new pricing system is going to be developed which will be even more efficient and better tailored towards the individual situation of every citizen. How is this possible? Luckily, our government is always keen to look at new technological developments and investigate how we, as citizens, may benefit from these. Consequently, innovative policy makers have suggested to implement a satellite-based road pricing system which will be able to tax us based on our actual usage of the Dutch roads. So, we will only pay for the products we use. A more honest and fairly divided system can hardly be imagined, or can it?"

This could be the testimonial of a government promoted advertisement for the new Dutch road pricing system which is due to be implemented starting 2011 (Ministerie van Verkeer en Waterstaat, 2008). We would almost be inclined to forget that, as clients of our government, we are not just consumers like in the private market. Citizenship is shaped by and shapes itself through power structures as vested in our democratic institutions. Law, politics and administration as well as the civil society and the media determine the multi-faceted nature of the government-citizen relationship. Consequently, citizenship has to do with constitutional and democratic rights and duties along with mutual dependencies of state and society.

[1] From 1985 to February 2009, Sjaak Nouwt was an assistant professor at the Tilburg Institute for Law, Technology, and Society (TILT) of Tilburg University. Currently, he is a policy advisor at the Royal Dutch Medical Association.

SDI Convergence. Research, Emerging Trends, and Critical Assessment. B. van Loenen, J.W.J. Besemer, J.A. Zevenbergen (Editors). Nederlandse Commissie voor Geodesie Netherlands Geodetic Commission 48, 2009.

The use of location-based information about citizens in public administration, such as the new road pricing system may affect the meaning of citizenship by shifting the information and the power relationship between government and citizens. Not only can LBS increase the governments' knowledge of who is where at what moment, the underlying technologies may also instigate the exertion of control of who goes where at what moment (Dobson and Fisher, 2003). Here, we address the inherent logic of LBS-applications in the context of Dutch public administration and aim at demonstrating the importance of the issue of privacy in public places.

In the next section we discuss in more detail the notion of citizenship in the information age. In the third section we focus on three LBS-applications in Dutch public policy, each of which are based on different positioning technologies. First, the introduction of a Radio Frequency Identification (RFID)-based public transport card is considered. Second, the plans for the new satellite-based road pricing system will be reviewed. Thirdly, we consider the use of mobile phone location data in crime fighting. We then present a model of the actors and data streams applying to location-based services in public administration and use this to reflect on the three cases. In section four of our contribution we discuss the concept of privacy in public places in relation to LBS as well as some relevant European case law.

2. CITIZENSHIP IN THE INFORMATION AGE

2.1 Citizens as subjects, clients and citoyens

Several scholars have argued that ICTs have the potential of altering the balance in the government-citizen relationship. The literature shows three extreme positions, which each indicate a different direction in which this relationship may evolve as a result of the ICT-revolution. The first two positions can be found in the Orwell-Athens debate as set out by Van de Donk and Tops (1992). The authors describe the scenarios of a powerful, Orwellian state on the one hand and that of democratic Athens-inspired society on the other. In each scenario different values regarding citizenship are dominant matching a different role the citizen can fulfil when interacting with government. In the Orwellian scenario, the citizen is predominantly treated as a *subject* of the state. Government has the power to set limitations on the behaviour of citizens and make sure that they obey the will of the state. The increased transparency of the citizen, caused by ICT, only helps government in steering and controlling society. Any deviant behaviour can be detected and acted upon using technological devices. Government thus uses ICT as a weapon to exercise power over citizens. In the opposing Athens scenario citizens seem to become more powerful thanks to ICT. They manifest themselves as *citoyens* in their relationship with government. In this role, citizens are treated as partners in the process of public policy making. Their opinions matter and now they can be consulted more easily than ever before thanks to ICT. The ideal of direct democracy is realised in Athens. As *citoyens* citizens have the right to get involved in public matters. In the Athens scenario, this right becomes reality.

Another debate in e-government literature shows us a third extreme position. Taylor et al. (2009) distinguish studies of the 'surveillance state' and studies of the 'service state'. The first type of studies are generally inspired by the fear of an Orwellian state, we already presented earlier as a first extreme position. The latter add a third perspective, which Frissen (1998) labelled 'Soft Sister'. As a Soft Sister, government emphasises the role of the citizen as a *client*. Government's top priority is to provide multiple and excellent services to its clients. As a *client,* the citizen expects and demands a certain service level when interacting with government. ICT opens new ways to cater

SDI Convergence. Research, Emerging Trends, and Critical Assessment. B. van Loenen, J.W.J. Besemer, J.A. Zevenbergen (Editors).
Nederlandse Commissie voor Geodesie Netherlands Geodetic Commission 48, 2009.

for these needs by increasing the quantity and quality of public services as well as tailoring these to the desires of the individual *client*. Government uses ICT as a tool to act in favour of citizens. At the same time, Soft Sister appears to be a different presentation of Big Brother.

When we use government services, there is no option to choose a different service provider. Moreover, usually we cannot withdraw from using government service because it is obligatory by law. In the Netherlands, for example, all citizens above the age of fourteen must, when asked by a police officer, identify themselves with an official identification document. In order to comply with this duty, Dutch citizens are obliged to use a government service to provide them with documents like passports or ID-cards. We are not clients of government in the same sense as being customers of private enterprises, because we are not free to choose whether we want to use a service or who we want to enjoy the service from. Consequently, we are always both *subjects* and *clients* of the state at the same time. Therefore, a holistic perspective in both research and practice of information-intensive government is highly desirable (Taylor et al., 2009).

2.2 The conscience of technology

The three citizen roles of *subject*, *citoyen* and *client* each emphasise different aspects of citizenship which are all important for governance in a democratic society. The three scenarios of Orwell, Athens and Soft Sister are extreme positions, which show the conflicting values government has to deal with when using ICT in interactions with citizens. Government ought to respect all three citizen roles and address citizens as such. However, we cannot count on technology itself to make the proper judgement and adapt its functionalities to the context it is used in. In other words, citing Davis (2003, in Michael et al., 2008), "technology has no conscience of its own". This does not imply, however, that technology would be a neutral tool, serving as a mere means to reach governmental goals. We would rather state that the characteristics of a particular technology convey an inherent logic which ought to be taken into account when applying it in interactions with citizens. What then, is the inherent logic of location-based services? This question will be explored in the next section by discussing three applications of LBS in Dutch public administration. We will demonstrate that despite the different underlying technologies, a similar pattern can be distinguished revealing the inherent logic of LBS.

3. LOCATION-BASED SERVICES IN DUTCH PUBLIC ADMINISTRATION

3.1 Three cases of LBS in Dutch public policy

3.1.1 Satellite technology for road pricing

In December 2007, the Dutch Ministry of Transport, Public Works and Water Management announced the Cabinet's decision to implement a new pricing system for the use of public roads (Ministerie van Verkeer en Waterstaat, 2007). According to the plan, by 2012, car drivers will be charged a price per kilometre. To implement this new system, the Dutch government will be using the latest satellite technology to collect location information about every car. Even though the legal, political and technological specifications have not yet been entirely determined, it is evident that the gathered location information will need to be connected to personal data in order to be able to send the right bill to the right person. Of course, the underlying report mentions that considerations about people's privacy will be taken into account when developing the system. Already, a private company has offered the responsible Minister a technological solu-

SDI Convergence. Research, Emerging Trends, and Critical Assessment. B. van Loenen, J.W.J. Besemer, J.A. Zevenbergen (Editors).
Nederlandse Commissie voor Geodesie Netherlands Geodetic Commission 48, 2009.

tion which does not measure a person's exact route, but just the number and type of roads he or she drives on instead, thereby realising a lesser invasion of privacy (Pieper, 2007). Nevertheless, a rich database with up-to-date, accurate, precise information about activities on the Dutch roads will be available.

3.1.2 RFID in public transport

The introduction of a new chip-based system for public transport is a politically sensitive topic. The Dutch government has decided to push forward the plan to implement one public transport card which can be used nation-wide on the infrastructures of all suppliers (Teepe, 2008). In this system, at the start of a journey the traveller checks in by bringing the RFID-enabled card close to the card reader. At the place of destination, during check-out the appropriate fee will be charged to the electronic wallet in the card. One reason for implementing this system is to get a more honest distribution of income between the various public transport companies. At this moment, the system has already been implemented by local public transport providers in parts of the Netherlands.

3.1.3 Mobile phone localisation in criminal investigation

The local law enforcement of the Dutch city of Nijmegen used cell phones in March 2006 to find possible witnesses to a criminal act. Three-thousand people received a text message asking them to contact the authorities if they could provide information about the murder of activist Louis Sévèke (Nu.nl, 2006). These people were not selected because they lived near the crime scene or because they were acquainted with the victim. They were merely selected because of their location or, to be more precise, the location of their cell phones at the time of the murder. This technological possibility instigated their involvement in the police investigation. The local law enforcement requested these data from the telecom providers and consequently, was able to send the request for information to the given phone numbers, resulting in several reactions. Little is known, however, about the psychological and social effects of this type of message. What were reasons to respond or not respond to this police call? Did people feel curious, scared, spied on or perhaps important or even appreciated? More research into this matter is desired in order to be able to assess the wanted and unwanted consequences of this kind of LBS-application.

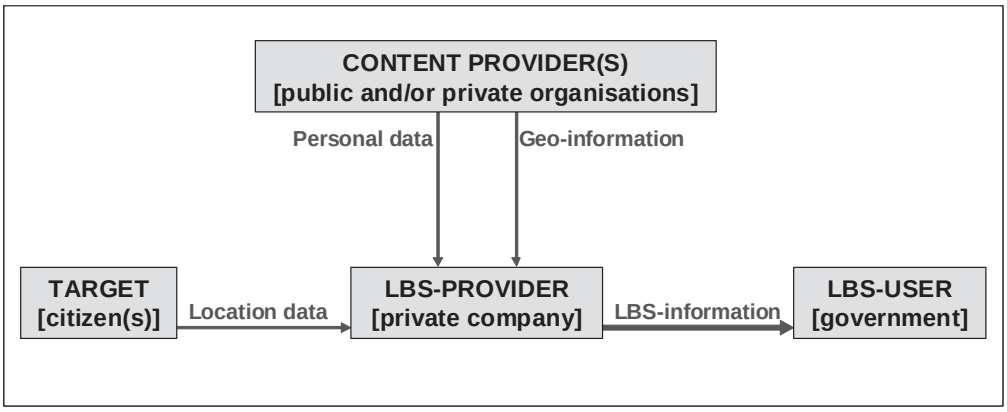
3.2 LBS logic

3.2.1 LBS actors and data streams

Location-based services are "IT services for providing information which has been created, compiled, selected or filtered taking into consideration the current locations of the users or those of other persons" (Küpper, 2005). Following this definition, generating information is the essence of LBS. Different positioning technologies can be used to do this. It follows that the LBS-user receives information based on his or her own location or that of other individuals. In the cases described in the previous section a government organisation places itself in the role of the LBS-user receiving information based on the location of citizens. For the technical realisation of LBS private parties play an important role as well. In addition, data streams from several other actors are also required for LBS. Based on Küpper's LBS supply chain (2005), Figure 1 is a possible visualisation of this situation.

SDI Convergence. Research, Emerging Trends, and Critical Assessment. B. van Loenen, J.W.J. Besemer, J.A. Zevenbergen (Editors).
Nederlandse Commissie voor Geodesie Netherlands Geodetic Commission 48, 2009.

Figure 1: LBS actors and data streams.



3.2.2 Citizens as targets

In this LBS supply chain, citizens are labelled as the *target*. The target is the actor whose position is determined by means of a positioning device. Technologically speaking, this actor is the starting point for LBS from the moment *location data* are generated. In the case of the public transport card information is transmitted as soon as the traveller's card finds itself near a RFID card reader. At that point, the card ID, the location of the reader and the time is first stored in a database belonging to the particular public transport provider and subsequently copied to a central database, thus containing the location data coming from all providers (Teepe, 2008). The road pricing system will use drivers' coordinates obtained from a satellite receiver placed in the vehicle. At this point it is uncertain whether these data will be stored in a device inside the vehicle or in an external database (Hoepman, 2008). In the Sévèke case location data in the shape of cell IDs were obtained from the potential murder witnesses as soon as their mobile phones were connected to the antennas in the area and these data were stored in the telecom providers' databases.

3.2.3 Personal data and geo-information as content

Another important data stream in the LBS supply chain consists of *personal data* about the 'targeted' citizens. In all three cases this is a relevant data stream. Regarding the public transport card, we see that people who currently have subscriptions or discount cards for their train or bus journeys automatically receive so called a personalised public transport card. This card's unique ID is linked to the subscribers' personal data as stored in, for example, the Dutch Railways' customer database. This organisation can thus serve as a *content provider* in the LBS chain. The argument is that this information is needed for authentication purposes (Teepe, 2008). A particular person's rights (to a discount) have to be linked to a particular card, literally opening the gates to the section that person is allowed to travel. In the case of road pricing, a similar reasoning is applicable, only in this case connecting a location device to a person's road tax paying duties. The third LBS case also requires personal data; this time it is a phone number so that they can be approached by a text-message. The telecom providers are the content providers of these data.

Other content providers, like Tele Atlas or Google may provide a stream of geo-information about the target's surroundings. Currently we do not know whether this will be the case in the examples mentioned here. However, we are aware of government and commercial LBS-applications where the use of GIS and geo-information plays an

SDI Convergence. Research, Emerging Trends, and Critical Assessment. B. van Loenen, J.W.J. Besemer, J.A. Zevenbergen (Editors).
Nederlandse Commissie voor Geodesie Netherlands Geodetic Commission 48, 2009.

important role (Dobson and Fisher, 2003; Ahas and Mark, 2005; Raper et al., 2007). GIS containing maps of the Rotterdam metro system, the Dutch road infrastructure and the neighbourhood of the murder could be the geo-information streams used in our examples.

3.2.4 Providing LBS-information to the government

The *LBS-provider* is the actor who integrates the aforementioned data streams. This actor collects location data about one or more targets, makes spatial analyses and combines this with other (geographical) data. The produced LBS-data are sent to the *LBS-user*. As such, raw location data are translated and enriched into LBS-information which can be read by the LBS-user. At this stage the previously collected personal data can be anonymised or pseudonymised and the location data may be aggregated if the LBS-user has no need for personalised detailed location data. This is the plan regarding road pricing. Even though the technological details on how to create the desired LBS-information are yet unknown, it is clear that the Dutch government has expressed its interest in this kind of aggregated data (Hoepman, 2008). As far as the public transport card is concerned, government interest in the collected data may come down to anti-terrorist or for crime fighting purposes (Van 't Hof, 2007; Teepe, 2008). However, it is yet unknown whether actual interest in this direction has been shown. The telecom providers in the murder case play the role of content provider as well as LBS-provider. The list of phone numbers belonging to the mobile phones which were localised in the neighbourhood of the crime scene around the time of the murder was obtained from LBS-information which the Nijmegen police force (LBS-user) received.

3.2.5 LBS-information: more and less

It is important to emphasise that LBS-information does not consist of the sum of the relevant location data, personal data and geo-information. It can be more and less at the same time. More, because of the added value to the government as the LBS-user, opening possibilities for analyses of large quantities of data and monitoring of citizens (Snellen, 2000). The result may also be less, because government may end with less detailed location information than initially collected or with (pseudo)anonymised data. In this respect private parties who play the role of LBS-provider are key actors because of the technological realisation of LBS. At the same time, government holds the power and responsibility to arrange for appropriate regulation deciding in which situations the LBS-information will be more or less than the sum of data streams.

3.3 Conclusion

We've seen that the core characteristics of LBS consist of collecting and synthesising data about citizens. These data are location data, personal data and geo-information connected to citizens. The possibilities the underlying technologies offer seem to be tempting to government organisations, especially in the field of intelligence. Whether government decides to use LBS-information to provide new services, create new democratic arrangements or monitor and control citizens, in all cases the initial data streams need to be acquired. Citizens always need to be targeted first in order to potentially benefit from new services or citizen participation. Looking at the aforementioned Sévèke murder case, it seems that the government wants to cooperate with the citizens – those who are witnesses – to solve the crime. Therefore, the government has a relationship with the citizen-citoyen. However, the same government also has the powers to relate the obtained information to possible suspects, for example when citizens do not cooperate for whatever reason. In that case, the government has a rela-

SDI Convergence. Research, Emerging Trends, and Critical Assessment. B. van Loenen, J.W.J. Besemer, J.A. Zevenbergen (Editors).
Nederlandse Commissie voor Geodesie Netherlands Geodetic Commission 48, 2009.

tionship with the citizen-subject. In other words, citizens are vulnerable in principle when LBS is concerned and find themselves in a weak position towards both the involved private parties and government. Therefore, at the starting point of LBS citizens are placed in the role of subject of the state. The government has legal powers to obtain location-based information about citizens. Obviously governments should be careful when collecting and using location-based information about citizens because it puts citizen trust in government at stake. Legal norms concerning a person's right to privacy in public places and data protection principles can help guiding governments through this pitfall.

4. PRIVACY IN PUBLIC PLACES

4.1 Definition of 'public place'

What distinguishes a private place from a public place seems obvious, but in 2004 this led, at least in the Netherlands, to discussions in parliament when the Bill on Camera Surveillance in Public Places was discussed (Kamerstukken 2004/5a). 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. 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, and
    - open sections of indoor shopping centres 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.

4.2 The opinion of the Dutch government

In the discussion of the Dutch Camera Surveillance Bill, the Christian Democratic Party (CDA) 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 relinquishes 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 (Kamerstukken, 2004/5b).

As we will show hereafter, this opinion obviously differs from that of the European Court of Human Rights (ECtHR), 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 (Hoge Raad, 1991), and concludes that

SDI Convergence. Research, Emerging Trends, and Critical Assessment. B. van Loenen, J.W.J. Besemer, J.A. Zevenbergen (Editors).
Nederlandse Commissie voor Geodesie Netherlands Geodetic Commission 48, 2009.

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 behaviour is, the less the right to privacy will be an issue. So, according to the Dutch government, a citizen's behaviour can be less or more public. This also means that a citizen can expect less or more privacy.

4.3 Article 8 ECHR

The right to privacy protects our 'private and family life, home, and correspondence' (Article 8, paragraph 1 European Convention on Human Rights). These are the basic elements of our privacy. Therefore, it seems that the right to privacy is especially applicable to private places. However, nowadays these private places are not so private anymore: we store a lot of our personal data on our personal hard disks, laptops, Blackberries, or iPods; also a lot of personal information is stored on the servers of our Internet service provider or on Google's servers. It seems that Big Brother is not only watching us, but he also knows where we are, where we have been and probably even where we are going to. Thanks to the technical solutions for large scale collection and analysis of personal data, including geo-information (location data, whereabouts), law enforcement agencies can compare these data with so called risk profiles. As a result, the privacy of citizens (subject, client and citoyen) 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 (Vedder et al., 2007).

The second paragraph of Article 8, ECHR allows public authorities to interfere with the exercise of the right to privacy of an individual. Such interference is only allowed on two conditions, namely that (1) interfering is in accordance with the law, and (2) interfering is necessary in a democratic society in the interests of:

- national security;
- public safety;
- the economic well-being of the country;
- the prevention of disorder or crime;
- the protection of health or morals, or
- the protection of the rights and freedoms of others.

An interference is in accordance with the law when it is allowed by legislation or by case law, as long as it is transparent for the citizen. An interference is necessary in a democratic society when there is a pressing social need to reach a certain goal while interfering with the right to privacy. "Necessary" means that the measure is appropriate to reach that goal (proportionality) and that no alternative measures are available that could also be appropriate (subsidiarity).

In the following subsection, we will analyse how the European Court of Human Rights (ECtHR) has recognised the right to privacy in public places. We will discuss two important cases in this respect: *Rotaru v. Romania* (ECtHR, 2000) and *P.G and J.H. v. The United Kingdom* (ECtHR, 2001). Other cases with regard to privacy in public places are e.g. *Peck v. The United Kingdom* (ECtHR, 2003a) and *Perry v. The United Kingdom* (ECtHR, 2003b).

SDI Convergence. Research, Emerging Trends, and Critical Assessment. B. van Loenen, J.W.J. Besemer, J.A. Zevenbergen (Editors).
Nederlandse Commissie voor Geodesie Netherlands Geodetic Commission 48, 2009.

4.4 European case law

4.4.1 Rotaru v. Romania

In 2000, the European Court of Human Rights passed an important judgment on the difference between private and public places in the case of *Rotaru v. Romania* (ECtHR, 2000). 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 (Ibid, § 44.). 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" (Ibid, § 43).

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.

4.4.2 P.G. and J.H. v. The United Kingdom

In the case of *P.G. and J.H. v. The United Kingdom* (ECtHR, 2001), 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 apartment, and that, while they were at the police station, listening devices were used to obtain voice samples.

The most relevant domestic law consisted of the Telecommunications Act 1945 and the Data Protection Act 1984. Section 45 of the Telecommunications Act prohibits the disclosure by a person engaged in a telecommunications system of any information concerning the use made of the telecommunications services provided for any other person by means of that system. However, section 28(3) of the Data Protection Act 1984 reads: "Personal data are exempt from non-disclosure provisions in any case in which – (a) the disclosure is for any of the purposes mentioned in subsection 1 above; and (b) the application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned in that subsection." Subsection 1 refers to data held for the purpose of: "(a) the prevention or detection of crime; (b) the apprehension or prosecution of offenders; or (c) the assessment or collection of any tax or duty." In this case, the Court concluded that the disclosure to the police was permitted under the relevant statutory framework where necessary for the purposes of the detection and prevention of crime (Ibid, § 47).

However, in the Court's opinion, there is also an area, even 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'" (Ibid, § 56).

SDI Convergence. Research, Emerging Trends, and Critical Assessment. B. van Loenen, J.W.J. Besemer, J.A. Zevenbergen (Editors).
Nederlandse Commissie voor Geodesie Netherlands Geodetic Commission 48, 2009.

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 (…)" (Ibid, § 57).

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.

4.5 Data protection principles

In the context of LBS, most of the time location data will be collected that can be related to identified or identifiable citizens. In such cases, the data protection legislation will be applicable. Apart from the question whether citizens can have a reasonable expectation of privacy, the 'controller' (in this case: the government) will have to comply with these data protection rules. The data protection framework is based on a number of general data protection principles. The basic data protection principles were formulated in the OECD Privacy Guidelines in 1980 and in Council of Europe Data Protection Treaty (Convention 108) in 1981. These traditional data protection principles still determine the framework for the fair and lawful processing of personal data, also with regard to LBS. The following general principles can, for example, be found in the Dutch Personal Data Protection Act (Hooghiemstra and Nouwt, 2007):

- processing of personal data must be fair and lawful and in accordance with the law;
- personal data are collected only for specified, explicit and legitimate purposes;
- processing of personal data must be based on legitimate legal grounds (e.g. the consent of the data subject or necessary for the performance of a contract);
- further processing of personal data must be compatible with the purposes for which the data were originally collected;
- personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access;
- personal data are kept no longer than is necessary for the purposes for which they were collected or for which they are further processed.

SDI Convergence. Research, Emerging Trends, and Critical Assessment. B. van Loenen, J.W.J. Besemer, J.A. Zevenbergen (Editors).
Nederlandse Commissie voor Geodesie Netherlands Geodetic Commission 48, 2009.

Without prejudice to the general data protection legislation, it is possible that special data protection legislation is applicable, for example for police data. However, this has no influence on the applicability of the general data protection principles.

Technical possibilities for large scale collection and analysis of personal data, including spatial data and telecommunications data make it much easier, for example, for law enforcement agencies to compare these data with so called risk profiles. As a result, the privacy of groups of citizens is at stake 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 (Nouwt, 2008; Vedder et al., 2007).

5. CONCLUSIONS

Legal norms are important for governments to demarcate the borders for collecting and using location-based information about citizens without interfering with their right to privacy. For some politicians, it is obvious that citizens have less reasonable expectations of privacy in public places. However, from ECtHR case law, we can conclude that the right to privacy also exists in public places where citizens can be monitored and information about them can be collected. From a legal perspective, governments are only allowed to collect location-based information about citizens when the powers to do so are in accordance with the law and there is a pressing social need to collect this information. Furthermore, collecting and further processing of personal data must be in accordance with the general data protection principles. Legal guidelines, however, are not sufficient to give direction to socially desirable applications of LBS in public policy (Onsrud, 2008). Governments should be critical towards the policy and societal goals they wish to attain by using LBS. When interacting with citizens, they should be aware of the conflicting values of the subject, citoyen and client role in order to avoid the extremes of Orwell, Athens and Soft Sister.

REFERENCES

Ahas, R. and U. Mark (2005). Location Based Services-New Challenges for Planning and Public Administration? *Futures*, 37(6): 547-561.

Dobson, J.E. and P.E. Fisher (2003). Geoslavery - Society Must Contemplate a New Form of Slavery, Characterized by Location Control, *IEEE Technology & Society Magazine: a Publication of the IEEE Society on Social Implications of Technology*, 22(1): 47-52.

Council of Europe (1981), Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&DF=8/27/2008&CL=ENG.

Davis, B. (2003). “Technoism: will loss of freedom unleash the voice of dissent?”, *International Symposium on Technology and Society: Crime Prevention, Security and Design, September 26-28 2003,* pp. 19-24.

ECtHR (2000). Rotaru v. Romania: European Court of Human Rights, Judgment of 4 May 2000, no. 28341/95, at: http://www.echr.coe.int/echr/.

ECtHR (2001). P.G. and J.H. v. The United Kingdom: European Court of Human Rights, Judgment of 25 September 2001, no. 44787/98, at: http://www.echr.coe.int/echr/.

SDI Convergence. Research, Emerging Trends, and Critical Assessment. B. van Loenen, J.W.J. Besemer, J.A. Zevenbergen (Editors). Nederlandse Commissie voor Geodesie Netherlands Geodetic Commission 48, 2009.

ECtHR (2003a). Peck v. The United Kingdom: European Court of Human Rights, Judgment of 28 January 2003, no. 44647/98, at: http://www.echr.coe.int/echr/.

ECtHR (2003b). Perry v. The United Kingdom: European Court of Human Rights, Judgment of 17 July 2003, no. 63673/00, at: http://www.echr.coe.int/echr/.

Frissen, P.H.A. (1998). "Public Administration in Cyberspace: A Postmodern Perspective", in Snellen, I.Th.M. and W.B.H.J. van de Donk (Eds.), *Public Administration in an Information Age. A Handbook*, Amsterdam/Berlin/Oxford/Tokyo/Washington DC: IOS Press, pp. 33-46.

Hoepman, J.-H. (2008). Follow that Car! Over de Mogelijke Privacygevolgen van Rekeningrijden, en hoe die te Vermijden, *Privacy en Informatie*, 11(5): 225-230.

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

Hooghiemstra, T. and J. Nouwt (2007). *Tekst en Toelichting Wet Bescherming Persoonsgegevens*, Den Haag: Sdu.

Kamerstukken (2004/5a). "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.

Kamerstukken (2004/5b). *Kamerstukken II*, 2004/05, 29 440, nr. 6, p. 10.

Küpper, A. (2005). *Location-based Services: Fundamentals and Operation,* Chichester: Wiley.

Michael, M.G., S.J. Fusco and K. Michael (2008). A Research Note on Ethics in the Emerging Age of Überveillance, *Computer Communications*, 31(6): 1192-1199.

Ministerie van Verkeer en Waterstaat (2008). Wet op de Kilometerprijs naar Raad van State, at: http://www.verkeerenwaterstaat.nl/actueel/nieuws/wetopdekilometerprijsnaarraadvanstate.aspx.

Nouwt, J. (2008). Reasonable Expectations of Geo-Privacy? *SCRIPT-ed*, 5(2): 375-403.

Nu.nl (2006). Politie Blij met Resultaat SMS-Bom Sévèke. *Nu.nl/internet*, at http://www.nu.nl/news.jsp?n=697945&c=50&rss.

OECD (1980), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, at: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

Onsrud, H.J. (2008). Implementing Geographic Information Technologies Ethically, *ArcNews Fall 2008 Issue*, at: http://www.esri.com/news/arcnews/fall08articles/implementing-gi-technologies.html.

Pieper, R. (2007). Anders Betalen voor Mobiliteit met Mobimiles. Brief aan Minister Eurlings 18 September 2007, ROAD Group.

Raper, J., G. Gartner, H. Karimi (2007). A Critical Evaluation of Location Based Services and their Potential, *Journal of Location Based Services*, 1(1): 5-45.

Snellen, I.Th.M. (2000). Territorialising Governance and the State: Policy Dimensions of Geographic Information Systems, Information Infrastructure and Policy: an International Journal on the Development, Adoption, Use and Effects of Information Technology, 6(3): 131-138.

SDI Convergence. Research, Emerging Trends, and Critical Assessment. B. van Loenen, J.W.J. Besemer, J.A. Zevenbergen (Editors).
Nederlandse Commissie voor Geodesie Netherlands Geodetic Commission 48, 2009.

Taylor, J.A., A.M.B. Lips and J. Organ (2009). Identification Practices in Government: Citizen Surveillance and the Quest for Public Service Improvement, *Identity in the Information Society,* 1(1).

Teepe, W.G. (2008). In sneltreinvaart je privacy kwijt, *Privacy en Informatie*, 11(5): 217-224.

Van de Donk, W.B.H.J. and P.W. Tops (1992). "Informatisering en Democratie: Orwell of Athene?", in Frissen, P.H.A., A.W. Koers and I.Th.M. Snellen (Eds.), *Orwell of Athene?: Democratie en Informatiesamenleving*, Den Haag: Sdu, pp. 31-74.

Van 't Hof, C. and R. van Est (2007). *RFID: Meer Keuze, Gemak en Controle in de Digitale Publieke Ruimte*, Den Haag: Rathenau Instituut.

Vedder, A., J.G.L. van der Wees, B-J. Koops and P. de Hert (2007). *Van Privacyparadijs tot Controlestaat? Misdaad- en Terreurbestrijding in Nederland aan het Begin van de 21ste Eeuw*, The Hague: Rathenau Instituut, Study 49 (summary in English), at: http://www.rathenau.nl/showpageBreed.asp?steID=1& ID=3814.

SDI Convergence. Research, Emerging Trends, and Critical Assessment. B. van Loenen, J.W.J. Besemer, J.A. Zevenbergen (Editors). Nederlandse Commissie voor Geodesie Netherlands Geodetic Commission 48, 2009.

SDI Convergence. Research, Emerging Trends, and Critical Assessment. B. van Loenen, J.W.J. Besemer, J.A. Zevenbergen (Editors).
Nederlandse Commissie voor Geodesie Netherlands Geodetic Commission 48, 2009.