In: National Security: Institutional Approaches… ISBN: 978-1-60876-893-6
Editors: Nelson J. Patten et al.

Chapter 2

BALANCING LOCATION PRIVACY WITH NATIONAL SECURITY: A COMPARATIVE ANALYSIS OF THREE COUNTRIES THROUGH THE BALANCING FRAMEWORK OF THE EUROPEAN COURT OF HUMAN RIGHTS

Bastiaan Van Loenen*[*]*, Jaap Zevenbergen and Jitske De Jong
Delft University of Technology, OTB Research Institute for Housing, Urban and Mobility Studies, Jaffalaan 9, 2628BX Delft, the Netherlands

ABSTRACT

Location based services (LBS) are among ICT developments that potentially put the privacy of individuals at risk. LBS technology allows for tracking and tracing the location of mobile phones or other terminal equipment. The increased possibility to know people's whereabouts, both in a geographical and temporal sense, is posing the question of possibility versus desirability with regard to location privacy. The central question that this article aims to answer is how may location privacy needs of cell phone users be balanced with national security needs of society? Through a study of literature and rulings of the European Court of Human Rights a balancing

[*] Corresponding author: Tel.: ++31(0)152782554; Fax: ++31(0)152782745;
Email: b.vanloenen@tudelft.nl,

framework was developed. The framework allowed for the assessment of the situation in the Netherlands, Germany and Canada with respect to the location data from mobile devices used by intelligence and security agencies to protect the national security. The research shows that the balancing should account for the totality of the circumstances. As for general interferences with the right to privacy also interferences with location privacy are very context-sensitive. A true balancing should be accomplished on a case-by-case basis. It is not a priori to be determined whether and to what extent location privacy is at stake. In all case studies similar requirements were found that should be taken into account in the decision what means to use in which instances. From the available published data, we expect that the use of these means varied among the case studies significantly, however. A proper balancing strongly builds on the balancing process, especially when balancing is very context-sensitive. This process should be just with adequate safeguards against abuse.

Keywords: Balancing framework; Location privacy; National security; Mobile devices.

1. INTRODUCTION

The issue of privacy protection is raising discussion in society, every time certain ICT developments allow for or simplify the collection, combination or application of new sets of person related data. Location based services (LBS) are among these relatively new ICT developments that potentially put the privacy of individuals at risk. LBS technology allows for tracking and tracing the location of mobile phones or other terminal equipment, for example car navigation systems. These are widely available and becoming increasingly precise in defining a location, opening new possibilities for government and commercial use of location information. Information about people's whereabouts, especially in combination with existing location information about a person (see De Jong et al., 1997), may reveal detailed information about personal profiles, relationships, and other aspects of personal life. The increased possibility to know people's whereabouts, both in a geographical and temporal sense, is posing the question of possibility versus desirability with regard to location privacy.

This paper addresses location privacy in the context of national security. The central question that this paper aims to answer is how may location privacy needs of cell phone users be balanced with national security needs of society? In some instances the scope of the paper has been broadened to law enforcement since information on law enforcement is generally more readily available than

information on the practices of intelligence and security agencies. Special attention was provided to the rulings of the European Court of Human Rights on the balancing of privacy and national security interests.

A case study was used to apply a balancing framework to the existing balancing practices in three countries: the Netherlands, Germany and Canada. These were performed through literature studies on the current legislation, and court rulings on privacy and national security. Confirmation with the findings was sought through interviews with knowledgeable experts. These interviews were partly carried out through email communications.

Focus of the research underlying this paper was on the Netherlands. Germany and Canada were selected since these are comparable to the Netherlands with respect to socio-economic development, but were assessed by Rothenberg and Knight (2004) and Rotenberg et al. (2006) to be countries with significant privacy safeguards in place. As opposed to the Netherlands which was assessed to have few privacy safeguards (Rotenberg et al., 2006).

A wide range of privacy enhancing technologies (PETs) are available to control access to the location information of mobile devices. However, since location information is a prerequisite for using the mobile device, it cannot be encrypted or otherwise withhold from intelligence or law enforcement agencies in the instance that these have a legal mandate to access the location data. Therefore, although these PETs may be sufficient to guard against private intruders, for law enforcement and security and intelligence services they are not. For balancing privacy and national security for provider controlled data, technology provides very limited opportunities to protect privacy. The balancing has then to be left to a decision in the extent to which technological advances may be used for national security purposes. The rulings of the European Court of Human Rights (ECtHR) provide such a balancing framework.

First, we will address the concept of privacy and location privacy. Then, we discuss national security in Section 3. Section 4 provides the balancing framework. Section 5 uses this framework to assess adherence or non-adherence to the balancing principles. It also addresses how in the case study the balancing between privacy and national security interests is performed.

2. PRIVACY

Most people would affirm the importance of privacy. However, the sense of what must be kept private differs from person to person. Privacy means different

things to different people (Westin, 2003, p.442). Some people love to give away their full personal life in TV shows or YouTube, while others are very reserved in providing their phone number or address.

Anyone may have some idea of what privacy means to him. Phrases that try to capture the concept such as 'My home is my castle', and 'The right to be let alone' (Warren and Brandeis, 1890, p.193; Cooley, 1880) are often used to indicate what privacy is.

However, the exact extent and meaning of privacy as a concept is difficult to capture in words because privacy is an elastic concept (Allen, 1988). Depending on one's perceptions different definitions of privacy may be developed. The attitude of individuals towards their privacy is also context-depending. Penders (2004, p.253) has explained this behaviour in the confidentiality of spheres. Within one sphere, for example the medical sphere, the work sphere, or private home sphere, data can be exchanged and in certain instances one expects that data is exchanged; e.g., the doctor exchanges your personal file with the hospital. However, many would object against exchanging personal data between spheres. For example, your doctor exchanging your medical file with your supervisor.

However, contexts may change and impact attitudes towards privacy (see Westin, 1967, 2003, p.433; Margulis, 2003). Koops and Leenes (2005, p. 149) foresee a significant impact of technology on location privacy expectations:

> "because technology is developing, so is the reasonable expectation of privacy surrounding technology. After all, there is less expectation of privacy when surfing the Internet than when watching television at home or walking streets that have clearly visible 24-hour camera surveillance. Likewise, the case of location data suggests that perhaps in the not too far-away future, people's movements may also lose the reasonable expectation of privacy since localisation is becoming an increasingly common side-effect of technology."

So not only individuals' perception, the dependency on context, but also time influences the extent to which the privacy is interfered.

Margulis (2003, p.415) found that many definitions of privacy share a common core of key elements. Key is control over transactions (interactions, communications) that regulate access to self and that as a result, reduce vulnerability and increase decisional and behavioural options (Margulis 2003, p.415). From a more practical standpoint, privacy is the "voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or a small group intimacy or, when among larger groups, in a condition of anonymity or reserve" (Westin 1967, p.7).

2.1 The Limited Access Approach

The limited access approach is widely used to utilise the concept of privacy (see, for example, Westin, 1967; Altman, 1975; Gavison, 1980; Mell, 1996; Walters, 2001; Camp and Osorio, 2002; Margulis, 2003, p.416). It discusses how individuals and groups control or regulate access to themselves (Margulis, 2003, 416). It reflects the individualist cultural model of the individual that prevails in western societies such as the US and Europe (Margulis, 2003, p.425). Controlling or regulating access to oneself can be divided in four types of privacy rights (cf. Sietsma, 2007, p.21; Walters, 2001, p. 10; Camp and Osorio, 2002, p.8-9; IPTS, 2003, 170; Koops and Leenes, 2005; Banisar, 2002; EPIC and PI, 2002, p.3):

1. Privacy of the body, which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches;
2. Privacy of the mind or psychological privacy; privacy as a right to have freedom to think and keep information which one does not want to reveal for himself: limited access to one's thoughts and state of mind.
3. Territorial privacy, or privacy in private places, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.
4. Behavourial privacy; privacy as a right to have freedom to behave as one likes.

Behavourial privacy can further be categorised in:

(a) Physical privacy; privacy as a right to have freedom of movement: a state or conditions of limited physical access to a person;
(b) Informational privacy; privacy as a right to control access to and dissemination of information about oneself: limited access to one's personal information, and
(c) Privacy of communications.

Location information involves aspects of behavourial privacy. Bodily, and psychological privacy remain unaddressed in this paper. Territorial privacy is only

addressed if this appears to be relevant. This may be in instances where an event or behaviour takes place at a certain (sensible) location.

2.2 Location Privacy

Location information provides the position of someone or something at a certain point in time and with certain accuracy. It links place, time, and attributes. Some attributes are physical or environmental in nature, while others are social or economic (Longley, 2001, 64-65). Location information may refer to the direction of travel, or to the identification of the network cell in which terminal equipment is located at a certain point in time (Directive 2002/58/EC).

Location privacy may be defined as the ability to control the extent to which personal location information is being used by others. In the context of mobile devices, location privacy is "the ability to prevent other parties from learning one's current or past location" (Beresford and Stajano, 2003).

The linkage of information to the earth makes the object or subject easy to identify, and as a result easy to reach, and/ or to determine the relative position between two devices. With data about a person's past and present locations, it is possible to impute aspects of the person's (future) behaviour. Moreover, linking the data of multiple people reveals human interactions, and behaviour patterns of groups (Clarke, 2001, p.208). In this way the location of a user provides important information to grasp the context of the user (Lee et al., 2005, p.1006). Location information is also valuable for location-based services because it implicitly conveys characteristics that describe the situation of a person (Gruteser and Grunwald, 2004, p.13).

Location information of mobile devices may also be useful for law enforcement or security and intelligence services; who was where at the time of the crime, where did he go, with whom and where is the suspect now (see, for example, Data Retention Directive 2006/24/EC, recital 11). Further, it may reveal the personal networks of suspects. In addition, location information could easily facilitate data mining and discrimination, leading to a surveillance situation where the control could even be performed by machines (IPTS, 2003, p. 66). Within a geographic context, privacy limitations will typically apply to the datasets with a high level of detail where, for example, individual houses or addresses can be used to reveal information about individuals.

2.3 Location Privacy Perceptions

Several researches have addressed the behaviour of people when using location based services. How private do individuals consider 'their' location information as private information?

Verhue (2007) has found that 'location determination through cell-phone' is considered to interfere highly with respondents' privacy. It was found to be at the same level as 'precautionary body search'. One might suspect that people using a mobile device would behave accordingly.

However, several researchers found that people are generally location privacy reluctant especially if they are provided in return with services that they consider useful (see Danezis et al., 2005; Cvrcek et al., 2006; Krumm, 2007; Chang et al., 2006; Kaasinen, 2005; Barkhuus and Dey, 2003; Colbert, 2001; Barkhuus, 2004; Ludford et al., 2006).

Further, some foresee an increasing demand for more detailed services (see Smith et al. 2003). ABI Research (2006) predicts a prosperous future for LBS with users subscribing to LBS services worldwide increasing from 12 million in 2006 to over 300 million in 2011. A study by JupiterResearch (2007) revealed that 45% of the surveyed parents with children under the age of 13 were interested and willing to pay for services that can keep track of their children.

These researchers suggest that the privacy expectations of users of mobile devices may not be as high as one may expect. It may very well be that these users are unaware of the potential privacy intrusions, or do not have a way of verifying or foreseeing what is being done to their personal data (see Barkhuus, 2004).

2.4 When Interference with Location Privacy?

At least three aspects determine whether there is an interference with location privacy:

- the type of information;
- the context of the location information;
- the timeliness of the location information.

2.4.1. Type of information

The category 'type of location information' stems directly from EU legislation (Directive 95/46/EC). Three categories are distinguished: (1) sensitive personal information, (2) personal information, and (3) non personal information.

The first category, sensitive information, includes information that is in itself considered to be sensitive such as health information. These are the 'special categories' of information, the processing of which requires special rules under Article 8 of EU Directive 95/46/EC (see also EC Regulations No 45/2001; art. 6 Convention 108). The second category, personal information, relates to information directly or indirectly identifying individuals. Examples of such information are the identifying information, such as a someone's name or an (IP-, email-) address indirectly identifying an individual. Finally, non-personal information does not interfere with privacy.

Generally, highly detailed location information would easily qualify as personal information. A small-scale dataset, e.g., a digital map of the world, is of such limited detail that it does not provide the ability to link the information to individuals: privacy issues are not likely to limit the use of small-scale information.

2.4.1.1. Type of location information in mobile devices

Although the user of the mobile device is not necessarily the person registered as the owner of the device, most information related to the mobile device can be relatively easily linked to an individual, which makes it personal data. This also applies to the location information involved.

Mobile devices inhibit several different types of location information. The differences concern the level of detail of the location information, the timeliness of the information, as well as the use mode of the device.

2.4.1.2. Location data v. traffic data

Directive 2002/58/EC distinguishes two types of location data: traffic data and location data. Traffic location data is necessary to enable the transmission of the communications. It may not necessarily be considered personal data since its accuracy varies from a 100 meter in urban areas to several kilometres in rural areas. In the context of the Directive (2002/58/EC) traffic data only applies to the location of the cell-phone at the moment the communication starts and the location of the cell-phone when the communications ends.

Location data are data that are more precise than is necessary for the transmission of communications (Directive 2002/58/EC, recital 35). Digital mobile networks may have the capacity to process such more precise location data.

Thus generally, traffic data is less accurate than location data. However, telecom providers are continuously improving the reliability of their network.

This includes an increasing number of telecommunication transmission towers which results in increased accurate traffic data.

2.4.2. Context of the location information

The level of detail may not always be decisive for the judgment of an interference with the right to privacy. Also the (ease to) link to a specific context is important. A combination of an address or a location of a mobile device, and other information can result in highly detailed and intimate personal data (see, for example, *R. v. Plant*). One may argue that revealing such data may impose a serious threat to the privacy of the individual that is linked to the device or address. For example, the device may be found frequently at the location of a mental hospital, which may suggest that the individual has a mental problem. Similar inferences can be drawn from visits to clinics, drugstores, coffee shops, tobacco shops, entertainment districts or festivals, political events, or ghetto areas with a criminal reputation (e.g., trailer home parks, scrap heap areas). Conclusions drawn from this information can interfere with the daily life of the individual (see also Gruteser and Grunwald, 2004, p.13). Linking location information to a 'sensitive' context will imply that the location information also should be treated as sensitive information.

The sensitivity of the location may also be related to one's profession, the characteristics of the location that could be identified, and other factors attributing to one's profile. For example, information that a Dutch citizen is calling from the Netherlands is not very informative. Information that a Dutch citizen is calling from Colombia might be informative, especially if it appeared to be the voice of a supposed member of FARC (a real Dutch example from 2007). However, if one's location does not have an impact on one's behaviour or performance in society, it can be considered non-personal data.

In addition, different users of the location information of another individual may have a potential different impact on that individuals' privacy perception. A different standard will be applied to family and friends than to direct marketing companies.

Another component not specifically being addressed in research or legislation is information on what one is doing somewhere. Westin (2003, p.445) suggests that the fact that it is known that one is at a certain location is less intrusive than the knowledge of what one is doing there (see Westin, 2003, p. 445).

2.4.3. Timeliness of location information

Time may have similar characteristics as location. The knowledge of what one is doing now may be considered private today. But twenty years from now,

this information might be irrelevant. In this respect, Cvrcek et al. (2006) found that location data of mobile phones extracted in the first month seems to be most valuable: "An observer gets a lot of information at the start of an observation period, such as their usual moving pattern. Subsequent months add very little information, and can therefore be seen as less valuable both from the point of the observer, and the person observed" (Cvrcek et al., 2006). This holds of course until the observed individual shows unusual behavioural patterns. For example, if he is frequently visiting a location near a nuclear power plant, or increasing the number of phone calls to certain people. These may indicate the preparations of a terrorist activity.

Generally, real-time location information is likely to be considered more sensitive than one's location in the past. In specific instances, however, this general guideline may not apply. For example, if old location data is linked to a specific expectation (e.g., at work), and it appeared that this expectation was falsified (e.g., with a mistress), the location information might be personal information. The cyclist Michael Rasmussen had a similar experience in the summer of 2007. He reported to be in Mexico prior to the Tour de France, but a former colleague cyclist saw him in Italy at the time he was supposed to be in Mexico. When this former colleague accidentally revealed this information, Rasmussen had to give up his number one position in the Tour de France and was fired. Thus, also linking rough location information to other information may result in a combined set of information that can be considered personal information.

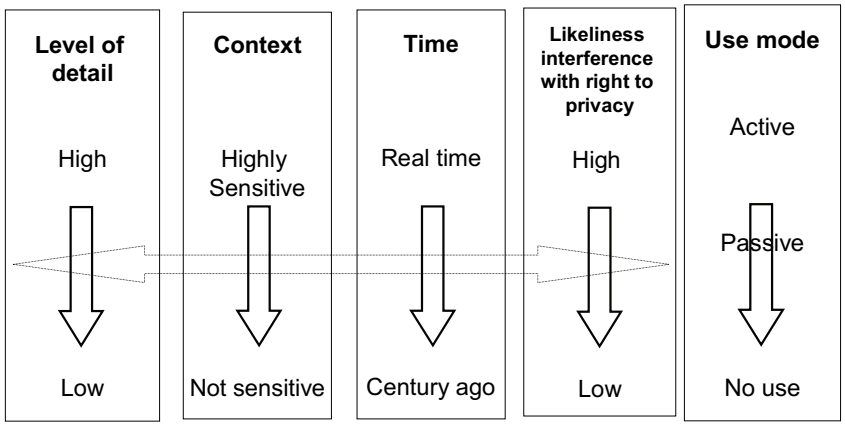


Figure 1. Factors determining the extent to which location information is interfering with the right to privacy.

2.4.4. Use mode: active, passive, or no use

Also the use mode of a mobile device may influence the extent to which the right to privacy is interfered with. We distinguished three types of use-modes: active use (e.g., calling), passive use (stand-by) and no use (device is turned off). The active use mode includes communicating with another device or individual. The user is aware that he is communicating with others. He even may be aware that his communications may be noticed by others. This is less likely for passive use. Mobile telephones in the standby mode may send transmissions to the local tower, enabling to track a person's movements (Clarke, 2001, p.213; see also Gruteser and Grunwald, 2004, p.15; Lee et al., 2005, p.1009). In addition, some cell-phones can be activated from a distance (McCullagh, 2006). For example, providers may install remotely software that may activate the microphone without the user's knowledge; so –called roving bugs (see *US v. Tomero*; McCullagh, 2006; Odell, 2005). Thus even if the cell-phone is in the standby mode, it may still be tracked down to a location. This may reveal information about the location the cell-phone is and its owner lives. For example, when the cell-phone 'sleeps' every night at the same location, where the address of the location may be referring to the address of its owner. One way of revealing secretly the location is SMS-ing the cell-phone periodically without ringing the ring-tone; a silent SMS (see *US v. Forest)*. The more active the use, the less infringing the interference with the right to privacy may be.

2.5 Summary

The type of location information, the context or the circumstances and timeliness determine whether location data may categorise as non-personal data, personal data, or sensitive personal data (see figure 1). The processing of location information may be among the most sensitive categories of personal information if it is linked to a sensitive context or if it is tracked and traced real-time. 'Historical' location information may fall in the general personal information category. A special regime may apply to the processing of historical location data of cell-phones in the stand-by mode. However, in specific instances a different categorisation may apply.

3. NATIONAL SECURITY

The concept of national security is difficult to define because it is closely related to subjective and sometimes emotional perceptions of administrations and military authorities about the threats to national security (Loof, 2005, p.235; see also Roberts, 2002). National security aims to protect a nation from internal and external factors threatening the continued existence of the norms that are the fundament of today's society. Therefore, a (democratic) constitutional state has the right to defend itself against intrusions on its (territorial) integrity including intrusions from other states, or against intrusions of the order of law within a state (Loof, 2005, p.105; see also Explanatory report of Convention 108). National security may be defined as the universal process of surveillance by authorities to enforce the rules and taboos of society (cf. Marx 2002, p.20; Westin, 1967, p.20; cf. Kamerstukken 28577 nr.3 p. 20; Kamerstukken 25877, nr. 58; UN Economic and Social Council *Siracusa Principles*).

National security is involved if an entire country, either territorial or its values, are threatened. The existence of the nation should not be limited to preservation of territorial and political independence from external armed attack, or dictatorial interference by foreign powers (Cameron, 2000, p.43 cited by Loof, 2005, p.245). It also encompasses espionage, economic or political, and covert (destabilising) action by foreign powers. Also internal threats to change the existing political order of the state by force (i.e. revolutionary subversion and terrorism) should be covered. With respect to internal threats, Coliver (1998, p.20) holds that it is not necessary that the threats erupt throughout the country, but their effects must be felt throughout, and the threats cannot be merely to the ruling party nor relatively isolated.

National security is typically protected by intelligence agencies that operate in strict secrecy. Also other parts of government may have a national security mandate, such as special law enforcement units or a national coordinator assigned to coordinate activities directed a protecting national security.

3.1 Timeliness of Society's Norms

Anyone supporting activities that are assessed to conflict with the norms of a society and potentially putting these norms at risk is likely to be subject to surveillance for reasons of national security. The elements threatening national security change throughout time. The norms change overtime and accordingly the subject of surveillance by intelligence agencies change. Throughout the centuries

in western society, the place of the devils and witches were exchanged for the heathen, for the unskilled workers, Jews, communists, and recently terrorists. For example, since the end of the cold war, supporters of communism are no longer considered a threat to the norms of society (see also Marx, 2002, p.17-18).

An example of a temporal change of norms within society is the change of the attitude after 9/11. Shortly after 9/11 54% of US citizens approved of expanded government monitoring of cell-phones and e-mails. One year later, September 2002, support for government monitoring of cell-phones and e-mail fell to 32% (Westin, 2003, 448). Also in the Netherlands public opinion was strongly influenced by shocking or news dominating events. In 2003, the invasion of US and UK armies into Iraq increased war concerns and in 2005 the assassination of Theo van Gogh had a similar impact on terrorism concerns (see Veldkamp, 2002, 2003, 2004, 2005; Verhue et al., 2006; Verhue, 2007).

3.2 Relevant Information to Protect National Security

Intelligence is an inescapable necessity for modern governments to address national security threats (Venice Commission, 2007, p. 1). In order to determine or prevent a (potential) threat the use of surveillance techniques may be necessary. Technology allowing surveillance, such as location technology, is increasingly important to protect national security. "[Surveillance] techniques can contribute to restrained and enlightened social control, helping to create a society orderly enough to enjoy its' freedoms" (Marx, 2002, p.22; Westin, 1967, p.19).

With respect to mobile devices, surveillance can be described as the purposeful, routine and systematic recording by technology of individual's movements and activities in public and private spaces (DPWP, 2006). It can be used to identify the risk-posing individuals and their networks (Mul et al., 2005, p.26). It is also important in verifying the statements or testimonies of victims, suspects, witnesses (Mul et al., 2005, p.26; Kamerstukken 2006-2007, nr. 31145 nr. 3 p. 9-10; Rotterdamse Politie, 2003, p. 6 of appendix), or to assess or confirm the reliability of an informant, although the legitimacy of such action is disputed in the literature.

4. BALANCING FRAMEWORK OF THE EUROPEAN COURT OF HUMAN RIGHTS IN ITS RULINGS

The right to privacy is in most international treaties recognised as a fundamental human right. The right is, however, not absolute. National security interests can justify a limitation to the right to privacy. This national security interest is acknowledged in all treaties as a legitimate purpose to interfere with one's privacy. The specific circumstances to interfere with the right to privacy depend on the specific case. Also national security needs do not automatically prevail over other interests. States may not, in the name of protecting national security, adopt whatever measures they deem appropriate (see *Klass*). As a practical fact, absolute privacy is difficult to accomplish, but absolute security may be as problematic to reach (see AIV, 2006, p.8). What is the proper balance between national security and privacy? (O'Harrow Jr., 2005, p.13; Westin, 1967; Margulis, 2001; Altman, 1975; Levi and Wall, 2004; Walters, 2001).

The (European) Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) is at the core of European privacy legislation. It addresses privacy in article 8:

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

The ECtHR's rulings on article 8 ECHR have developed a rather solid framework further specifying and explaining article 8. Article 8's Private and family life, home and correspondence relates to homes, but also offices and business premises, communication such as correspondence by mail but also telephone, fax and internet use, and thus covers telephone tapping, strategic monitoring, and storage of information, among others (Myjer, 2007). Data protection and privacy issues or aspects can also be found in the Articles 5, 6, 10 and 13 ECHR.

In the following section, we will introduce the general framework and its four principles. The following sections present these principles in more detail, and

include observations on the balancing practice in three countries (the Netherlands, Germany and Canada) we studied. A tabular overview in relation to principle 4 is supplied in the last section.

It should be noted that the ECtHR has rarely addressed location privacy in the context of mobile devices. However, the ECtHR has ruled consistently on the use of other privacy intruding means such as wiretapping. These requirements would also apply to the use of location technology for national security purposes.

An analysis of the judgments of the European Court of Human Rights, together with the European Convention of Human Rights, Convention 108 and OECD principles, results in four general principles that need to be satisfied to interfere with the right to privacy for purposes of national security (for details see Van Loenen and Zevenbergen, 2007):

Principle 1: Interference for national security purposes must have some basis in domestic law, law must be accessible to all, and the means of interference should be foreseeable for citizens.

Principle 2: A fair balance has to be struck between the demands of the general interest and the interest of the individual.

Principle 3: Interference should be proportionate to the legitimate aim pursued.

Principle 4: Interference is only allowed if adequate and effective guarantees against abuse exist.

It has been suggested that for balancing privacy and national security an equilibrium exist or can be accomplished (see Gerards, 2006). However, in the context of national security, it is not a matter of balancing national security and privacy with the suggestion of finding an equilibrium. If a national security threat can be assumed, then the balancing is a matter of interfering with the right to privacy on reasonable grounds and based on arguments that safeguard the right to privacy through adhering to the general privacy (and personal data processing) principles. Therefore, in attempting to strike a fair balance between national security and privacy, it is a matter of addressing the threat effectively and respecting the right to privacy to the greatest extent possible. Starting point in this section is that there is a need to address national security threats. Question is then what means to use, for how long, among others. Special focus is on the use of telecommunication data with respect to principles 1 to 4.

5. APPLYING THE PRINCIPLES: CASE STUDY RESULTS

5.1 Principle 1: Interference for National Security Purposes Must Have Some Basis in Domestic Law, Law Must Be Accessible to All, and the Means of Interference Should Be Foreseeable for Citizens

In the ECtHR's settled case-law, 'in accordance with the law' not only requires the measure to have *some basis in domestic law*, it should be adequately *accessible* to the person concerned and *foreseeable* as to its effects (see *Rotaru* §52). It also refers to the quality of the law in question: the law must be *compatible with the rule of law*; it must provide effective remedies against arbitrary interference by public authorities with the privacy rights of Article 8. This especially applies if the law provides (wide) discretionary powers to administrative or judicial forces (Loof, 2005, p.210). Article 13 of the Convention requires that these remedies are 'effective' in practice as well as in law (*Rotaru* §67).

Interference for national security purposes must have some basis in domestic law

Although generally broad and vague terminology is used to describe national security, in all cases national security is specified in law as a legitimate purpose to interfere with privacy. The Dutch security and intelligence agency is tasked to protect the core interests of the Netherlands, being among others the continuance of the democratic order or the security of the state or other major interests of the Netherlands. Its Canadian counterpart (Canadian Security Intelligence Agency, CSIS) is mandated to collect, analyse, and retain information and intelligence regarding activities that may pose a threat to the security of Canada. The German security and intelligence agency (BfV) is tasked to address efforts directed against the free democratic basic order, the existence or the security of the Federation or one of its States or aimed at unlawfully hampering constitutional bodies of the Federation or one of its States or their members in the performance of their duties, among others.

Accessibility of the law

In all case studies, the law is readily accessible.

Means of interference foreseeable

In all cases provides legislation the framework within which security and intelligence services are operating. Legislation establishes the means that can be utilised, and the information that can be used from third parties. In this way, it balances to a certain extent the needs of society and those of individuals.

In specifying what means of interference may be used (in what instances), the German and Dutch intelligence law are explicit in what means are available and which are not. For example, in Germany and the Netherlands, information on the location of a mobile device which is not actively used (standby) cannot be required from telecom providers for national security purposes. In Canada, it is specified that all means are available. It is upfront unclear which means may be used in what instances, and which means are not available. Common law in Canada, however, has provided more direction in what means are considered proportionate in what situations (see further under principle 3 section 5.3).

In some instances, practical reasons have led to the availability of certain data in one country while in other countries it may not be available. One example is the requirement in the European Union to store for at least six months traffic data of telecommunications (Data Retention Directive 2006/24/EC), while Canada lacks such requirement. There is in Canada, for telecommunication data, not a minimum standard data set that should be stored by telecom providers and there is no strict standard on minimum or maximum retention periods. In addition, in Canada, telecom service providers are not by law required to provide interception capability. In this respect, Canadian security and intelligence agencies cannot rely on the telecommunication providers' data as much as their European counterparts.

The European Court of Human Rights' foreseeability requirement requires that the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to resort to any such secret measures. However, in this research it has been argued that the more transparent the law is on the available means for specified circumstances (i.e., crimes) the more likely it is that these means are being used for these specified circumstances. Several interviewees independent of each other confirmed that increased transparency promotes the use of infringing means. Affirmation of this hypothesis would argue against the ECtHR requirements. Further research is required to test this hypothesis.

5.2 Principle 2: A Fair Balance Has to Be Struck between the Demands of the General Interest and the Interest of the Individual

Several requirements are a prerequisite for true balancing of privacy and national security interests. First, the process itself must be just, that is, "the interests of all are fairly represented'; and the outcome of the process must protect basic dignity and provide "moral capital for personal relations in the form of absolute titles to at least some information about oneself" (Walters, 2001, p.11).

Several relevant steps in the balancing process can be distinguished:

- assessing the need to address a potential national security threat (seriousness and urgency);
- assessing the availability of means to neutralise the threat;
- selecting the most effective means with the least impact on the right to privacy;
- selecting the most effective data with the least impact on the right to privacy, and
- establishing the safeguards for using the means such as review and complaint mechanisms

From all the available means, the most effective may be selected. Then, it needs to be assessed what the conditions need to be for using these means: what means may be used when, for how long, and what safeguards need to be respected, among others. If the selected means are telecommunications, the same questions will apply to the type of data to be used. The answers to these questions may vary from place to place, and from situation to situation. Data from the case studies is presented in the sections 5.3 and 5.4.

5.3 Principle 3: Interference Should Be Proportionate to the Legitimate Aim Pursued

According to the ECtHR's settled case law, a legitimate aim needs to be pursued, and there should be a "reasonable relationship of proportionality between the means employed and the aim sought to be realised" (*Marckx* §33, *Dudgeon* §53; *Norris*; *Belgian Linguistic case*). If the aim sought can be realised with

alternative less intrusive means, the ECtHR finds the intrusion disproportionate (*Olsson* §83, *Hatton* §97). This principle is also known as the subsidiary principle.

In circumstances of national security, the ECtHR has accepted that the margin of appreciation available to the respondent country in assessing the pressing social need, and in particular in choosing the means for achieving the legitimate aim of protecting national security, is a wide one (see *Leand*er §59; *Weber* §106).

5.3.1. Effective use of location data in law enforcement

This research has shown that a phone tap provides a quick and reasonable well picture of a criminal organisation. In this respect it is not the content of the communication that is most interesting, but the contact information: who is calling who. Phone call frequencies in that matter may be used to identify 'catch someone in the act' situations (Reijne et al., 1996). These are more important for law enforcement than precise location data. Historic traffic data is critical to reveal connections between suspects (Rotterdamse Politie, 2003, p.5). Location data of a cell-phone may be used to uncover a criminal network, but the other types of information can be more useful (Rotterdamse Politie, 2003, p.5).

Location data of a cell-phone can be very useful in complementing other special means, especially in supporting the observation means (see Van de Pol, 2006, p.139; HR 17 September 2002 LJN AE4200). The location component of the traffic data may be useful to some extent to identify the places a suspect visits, or has visited. It may further show behaviour indicating increased or decreased activity in a certain location. The location of a cell-phone may further be linked to events that took place in the past in the surroundings of that location suggesting that the cell-phone was at that specific time in that place. Linking cell-phone and event may result in new, previously unknown, suspects.

Also most interviewees see an advantage in using phone taps in combination with other investigative means, preferably with an observation team. Objective of observation is to identify participants of a supposed criminal organisation and the people with whom they maintain contact, the role of the participants within the network and the activities they perform within the network, especially concerning the transfer of certain things (for example, money or drugs) (Court of Appeal The Hague 25 January 2000 LJN AE0196).

It is unclear to which extent location information is a prerequisite to prevent urgent threats. Preventing a threat would likely require additional measures, including physical observation.

Data from cell-phones are not by definition reliable law enforcement means, however. Some suspects use this knowledge to give their cell-phone to their husband on the day of a robbery and use another (prepaid) cell-phone. This cell-

phone may then be destroyed directly after the robbery. The location data of a beacon does not do more than provide the location of the object – and for that matter not necessarily also of the subject – on which the beacon was placed (HR 17 September 2002 LJN AE4200; HR 10 December 2002 LJN AE9632; Kamerstukken 2001–2002, 28 059, nr. 3, p.8). Location data of a cell-phone provides some evidence of the presence of a device at a certain location at a certain time (see, for example, HR 7 September 2004 LJN AO9090). However, it is not necessarily the nearest telecommunication tower that is being used in the communications. It may very well be a BTS several kilometres away from the location of the cell-phone. In addition, in the Netherlands, only traffic data (i.e. information that is required for the phone bill) is stored. Thus, only the BTS used at the start of a communication and the BTS that is used at the moment of ending the communication are stored. The BTS-s used in between are not stored. Therefore, fully depending on the location data of a cell-phone for preventing a crime or for solving crimes is insufficient.

Location data of the cell-phone may be useful if combined with other information or means. Tactical information such as the address of friends, family, other suspects may be useful in combination with the location data of a cell-phone. The same applies to physical observation in combination with location data.

5.3.2. Subsidiary criterion: assessing an order of privacy interfering means

The ECtHR and all case study countries apply the subsidiary criterion. The subsidiary criterion rules that from the available appropriate measures, the one prospectively least restrictive for the data subject shall be used. Data from publicly accessible sources (like newspapers, flyers, programs, public events or government sources (e.g., police) are considered less infringing than other means of data collection. Thus, only if publicly or government accessible sources are insufficient (e.g., not timely available, unreliable, not available), special means may be used.

In Canada, the Canadian Security Intelligence Service (CSIS) needs to show that other investigative procedures have been tried and have failed or why it appears that they are unlikely to succeed. Further, the application should address that the urgency of the matter is such that it would be impractical to carry out the investigation using only other investigative procedures or that without a warrant it is likely that, in this specific context, information of importance will not be obtained.

In Germany, monitoring of individuals through telecommunications is permissible only if less intrusive means of investigation have no prospect of

success (*aussichtslos*) or are significantly more difficult (*wezentlich erschwert*). It may be regarded as the 'last resort' in investigating a catalogued crime or in locating the suspect. A 'last resort' situation may be assumed only if other investigative methods would be unsuccessful (Albrecht, 2006, p. 16). Also in the Netherlands the subsidiarity criterion exists. The Minister has pointed out, however, that it is difficult to assess the privacy infringement of available means compared to each other since this is case depending.

Proportionality and subsidiarity seem to be principles that are very context-specific and time-dependent. The content of these principles seems to differ with social and political developments (see Nouwt et al., 2004, p.354).

5.3.3. Effectiveness of means and subsidiarity in case studies

Concerning the effectiveness of means, we may take the number of phone taps as an example to compare differences of used means between case study countries. These numbers are only available for law enforcement. To provide some sense of the number of wiretaps in the case study countries we use these numbers. In the Netherlands, the total number of new tap orders for 2007 is likely to be in the range of 25 000 phone numbers (see Ministry of Justice, 2008). This equals 151 taps per 100 000 citizens. In Canada, the number of interceptions of telecommunication has dropped from 1 679 interceptions in 2002 (5.2 per 100 000 citizens) to 584 interceptions (1.8 per 100 000 citizens) in 2005 (Ministry of Public Safety, 2007). In 2006, the number of taps in Germany on cellphones was 35 816, and approximately 5 000 taps on traditional phones (Bundesnetzagentur, 2007). This amounts in approximately 50 taps per 100 000 citizens. Figure 2 shows the differences.

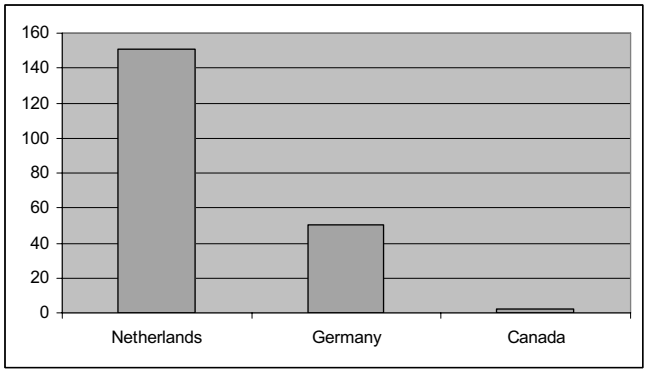


Figure 2. The approximate number of taps for law enforcement in the case-study countries per 100 000 citizens

These differences are difficult to explain, and raises the question whether some countries may relatively easy approve the use of one of the most privacy-intruding means: the phone tap. Do these countries truly balance law enforcement and national security interests of society with other critical interests of society? And are these means assessed to be more effective than alternative, but less privacy-infringing means?

5.3.4. Proportionality

The decision whether a selected means (i.e. data processing) is proportionate needs to address the following issues (based on Buruma, 2001, p.36; ECtHR rulings; Kamerstukken 98-99 25403 nr. 25, p.5; Kamerstukken 97-98 25403, nr. 7, p.47; Kamerstukken 1996-97 25403 nr. 3, p.27; Hoge Raad 21 March 2000 LJN AA5254; Hoge Raad 12 February 2002 LJN AD9222, O'Harrow Jr., 2005, p.139; Marx, 1998; Commissie van Toezicht, 2005, p. 37; *R. v. Duarte*; *R. v. Collins*; *Hunter*; *German Federal Constitutional Court* 1999; *GPS case*; Jacoby, 2005; *Rasterfahndung case*; *Weber*):

- What is the (intimacy of the) place (public road, home, office, church) to be observed?
- How will the observation be accomplished (technical means as camera's or beacons and their possibilities)?
- What will be the inconvenience for the observed person?
- What is the consecutive period of observation (hours, days, weeks)?
- What is the intensity (continuous, periodic or with intervals)?
- What accuracy standards will be used?
- What is the timeliness of the data?
- Who will use the acquired data?
- What guarantees are available to ensure that sensitive data will be protected against manipulation, theft or diffusion?
- What are the costs of using these means?

The longer the period of observation, the more intimate the place of observation, the higher the intensity or frequency of observation, the more accurate and timely the information, and the more possibilities the supportive means provide, the higher the chance that someone's privacy will be interfered with.

In one case, we have seen that avoidance strategies (disabling electronic beepers, evading tailing vehicles) may justify the use of more privacy intruding techniques or data (see Ross, 2005, p.1808 referring to *GPS case*).

Adherence to the proportionality requirement requires a case-by-case approach, which is difficult to model to the greatest detail. Especially the assessment of the privacy impact of the use location data is very context specific (see section 2). Therefore, it is difficult to provide a decisional framework in which a priori is decided what means are proportionate to use in which situations. Use of most intruding means would typically be reserved for most urgent threats. A privacy impact assessment (PIA) may be used to assess the privacy impact of several selected effective means. Canadian federal agencies are required to perform a privacy impact assessment for proposals for programs and services that raise privacy risks (Lemieux, 2007).

5.4 Principle 4: Interference is Only Allowed If Adequate and Effective Guarantees against Abuse Exist

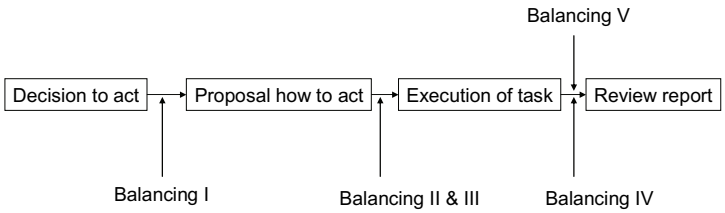
In the context of national security, privacy protection may be synonym with a just decision-making process and proper execution of the national security mandate. If the quality of this process is central in protecting privacy the question is then: how to ensure that the security and intelligence service is doing what it is supposed to do, no more and no less in a way that infringes fundamental rights the least? Organisational remits may prevent a situation in which authorities "take such liberties, in endeavouring to detect and punish offenders, as are even more criminal than the offences they seek to punish" (Westin, 1967, p.332). AIV (2006, p.52) argues that for the protection of fundamental rights the role of independent judges as the legal protectors of these rights is of eminent importance (see also ECtHR in *Klass;* UN, 2005, par. 13-15). In the cases, we see that independent authorities may have different roles. Figure 3 provides this conceptually for the decision making process to use special means, generally the most intrusive means, to protect national security. In each balancing step the interests of national security may be balanced with those of privacy.

5.4.1. Balancing III for telecommunication data: data from the case-studies

Table 1 summarises the required authority that needs to approve the requisition of telecommunication data in the case-study countries. It shows that each country has a different regime for information related to or concerning location.

In the Netherlands, no independent authority is involved in the decision to use special authorities by the intelligence and security agency. Only if the operations involve the content of communications, the Minister has to approve use of the measure. In Canada no distinction is made in the law between any type of information. Although the Federal Court might be likely to easier accept or require lower standards for requests concerning solely identification data compared to the full range of available telecommunications data, this was not confirmed in this research. Depending on the totality of the circumstances of a case, a greater or lesser reasonable expectation of privacy may be found. The expectation of privacy in private areas, i.e., the home, is greater than in public areas. In Germany, the decision model is most detailed developed in the law. The independent G-10 commission needs to approve the surveillance of traffic data and location data of mobile devices, putting these at the same level as the content of communications.

Stand-by information cannot be requested by the security and intelligence agencies in the Netherlands and Germany, while it can in Canada. Further, in all cases the processing of sensitive personal data appears to require a similar level of approval as identifying data. In Canada, this is the same high level of approval by the Courts. In Germany and the Netherlands, this is at the level of the security and intelligence service. This latter situation seems to ignore the universal understanding that these data are the most intimate personal data. In the Netherlands, the sensitiveness of data concerning political opinions, and trade-union membership is not represented in the approval hierarchy if to be processed by intelligence agencies; it requires the lowest level of approval.



Balancing I: initiative to start the process for selection and use of special means
Balancing II: decision to proceed with the process to obtain approval for use of special means
Balancing III: approval to use special means
Balancing IV: reactive or passive oversight of activities of intelligence and security agency
Balancing V: continuing overall active review of the operations of the intelligence and security agency

Figure 3. Conceptual view of decision making process.

Table 1. Sensitiveness of data based on required approval as specified in intelligence law in the Netherlands, Canada, and Germany (the darker the cell the higher the level of approval)

Type of data	Examples	Netherlands: Decision/ Requisition by	Canada: Decision/ Requisition by	Germany: Decision/ Requisition by
Identifying data	Name, address, phone number, kind of service used, IMEI-code, type of services used, identifying data of subscriber (paying the bill), bank account number	Head of security and intelligence service	Minister & Federal Court judge	Head of security and intelligence service
Traffic data	Historical and future location data of cell-phone if actively been used, date and time of use	Head of security and intelligence service	Minister & Federal Court judge	Minister & Independent commission
Content of communications	Conversation, content of an email or voice mail	Minister	Minister & Federal Court judge	Minister & Independent commission
Certain stored data: other data	(Historical and future) location data of cell-phone in stand-by mode processed by telecommunication provider	N/A	Minister & Federal Court judge	N/A
Data processed after requisition date and directly available	Real-time location data of cell-phone if actively been used	Head of security and intelligence service	Minister & Federal Court judge	Minister & Independent commission
Sensitive personal data (1)	Data concerning racial or ethnic origin, religious or philosophical beliefs, or concerning health or sex life	Head of security and intelligence service (Only allowed if inevitable)	Minister & Federal Court judge	Head of security and intelligence service
Sensitive personal data (2)	Data concerning political opinions, trade-union membership	Intelligence agent	Minister & Federal Court judge	Head of security and intelligence service

The detailed legislation in Europe may ignore the totality of the circumstances in the decision to use a special means such as a wiretap, or real-time tracking of an individual. This categorisation in law assumes that the right to privacy is a rather absolute concept which can be applied in the same manner, whatever the specific circumstances of a case may be. However, real-time location information may sometimes be considered very privacy sensitive

information, while the content of a nonsense conversation with a family member may not. In addition, in some instances it is very sensitive information with whom you communicated, no matter what was discussed or where it was discussed. These nuances may not be part of the decision-making procedure to use special means like wiretapping, or claiming location information. At least, they are not necessarily acknowledged in the hierarchy of the approval structure.

5.4.2. Balancing IV reporting use and effect of telecommunication data: data from the case-studies

To assess the effectiveness of available means, qualitative or quantitative data on the use and effect of these means are a prerequisite. Only Canadian law requires the CSIS to report yearly publicly the number of phone taps. In Germany and the Netherlands such a requirement does not exist for phone taps. In all cases, no obligation exists to report on the number of requests for traffic data, or location data of mobile devices. Therefore, information on the use of these data is scant; their effectiveness remains unassessed. Accordingly they, or the Minister cannot be held accountable for increases or decreases of the number of request for these data.

Such a situation results in non-informed decisions (in parliament) that may shift the balance between privacy and national security significantly. Politicians should be able to take a balanced view on these matters that not only may impact individual citizens in the short term, but might undermine the democratic values underlying our democratic society in the long run. They can only do this through informed decision making. Informed implies knowledge about the use and effect of current means, and the expected effect of proposed means.

Table 2. Balancing for use of real-time location information of mobile devices (active use; the darker the cell, the more independent the balancing)

	Balancing I	Balancing II	Balancing III	Balancing IV	Balancing V
Netherlands	Intelligence and Security Service	Intelligence and Security Service	Intelligence and Security Service	Ombudsman, Review Commission, Court	Independent review + parliamentary review
Canada	Intelligence and Security Service	Minister	Federal Court	Review Commission, Inspector General, Court	Independent review + parliamentary review
Germany	Intelligence and Security Service	Minister	Independent Commission	G 10 Commission, Court	Parliamentary review

In all cases, complaints on the security and intelligence agencies should be filed with the security and intelligence agency's review commission (balancing step IV). None of these, however, can render legally binding decisions. In all cases, complaints on the execution of the tasks may (ultimately) be directed at a (civil) court.

5.4.3. Balancing V continuing overall active review of the operations of the intelligence and security agency: data from the case-studies

Balancing V involves review for evaluation purposes. An evaluation purpose may be to periodically evaluate the available means and their necessity for the operations of the security and intelligence agency (see AIV, 2006, p. 8; see also Koops, 2006). Such an independent authority is required to oversee the execution of the activities of the security and intelligence services (Schmid, 2001). Review by an independent commission is found in Germany, Canada, and the Netherlands. In Germany, this independent commission is in a permanent parliamentary commission. In the Netherlands and Canada, this is in independent review commissions. None of the review commissions can render legally binding decisions. Parliamentary oversight is found in Germany, Canada, and the Netherlands for national security (see Table 2).

5.5.4. Balancing process in summary

Each country has some kind of independent oversight or review. In Germany and Canada independent authorities are part of the decision-making process: their approval is required to use the means (the balancing III step). The Netherlands has chosen for a system in which the decision-making is the responsibility of the security and intelligence service with political responsibility in the Minister of the Interior (or Defence for the Military Intelligence Service).

It should be noted that independent oversight and review can only be effective with adequate capacity, both qualitative as quantitative, in such body. In this respect, review and oversight mechanisms need to keep pace with developments in the national security sector to fulfil the review task adequately.

6. CONCLUSION

How far the right to privacy should reach with respect to the location data from mobile devices used by intelligence and security agencies to protect the national security depends on the totality of the circumstances. As for general

interferences with the right to privacy also interferences with location privacy are very context-sensitive. A true balancing should be accomplished on a case-by-case basis. It is not a priori to be determined whether and to what extent location privacy is at stake. In all case studies similar requirements were found that should be taken into account in the decision what means to use in which instances. From the available published data, we expect that the use of these means varied among the case studies significantly, however. A proper balancing strongly builds on the balancing process, especially when balancing is very context-sensitive. This process should be just with adequate safeguards against abuse.

The Canadian framework for deciding to use a special means, which is here telecommunication data, to neutralise a national security threat, meets the requirements of respecting the totality of the circumstances and adequate safeguards most adequately. The Canadian law does not specify which means or data could be used in what specific circumstances, but leaves this decision to an independent authority (Federal judge). The use of the special means is reviewed actively by an independent review commission, and information on the number and type of special means by the security and intelligence agency is published.

The potential impact of surveillance and the ever-changing needs of society provided, societies need to be reserved about providing intelligence services ubiquitous mandates to protect national security. Changing the law in favour of national security considerations based on time dependent threats needs to be a conscious well-balanced choice, which should not be taken overnight. Contrary to the transparency requirement of the European Court of Human Rights this research suggests that law describing the available means to protect national security in general terms will better respect the right to privacy then legislation describing in great details when to use what means. Additional research is required to evidence this hypothesis further.

ACKNOWLEDGEMENTS

This research has been accomplished under research grant 458-04-022 from the Dutch NWO program Netwerk voor Netwerken.

REFERENCES

ABI research. (2006). GPS-Enabled Location-Based Services (LBS) Subscribers Will Total 315 Million in Five Years.

AIV (Adviescommissie Informatiestromen Veiligheid). (2007). Data voor daadkracht; Gegevensbestanden voor veiligheid: observatie en analyse. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Albrecht, H. J. (2006). Counterterrorism policies in Germany. in: R. Neve, L. Vervoorn, F. Leeuw & S. Bogae (Eds.), Een eerste inventarisatie van contraterrorismebeleid: 'Policy and research in progress' in Duitsland, Frankrijk, Italië, Spanje, het Verenigd Koninkrijk en de Verenigde Staten (A first inventory of counterterrorism policy: policy and research in progress in Germany, France, Italy, Spain, the UK and the US). WODC, Den Haag.

Allen, A. (1988). *Uneasy Access: Privacy for Women in a Free Society*. Rowman and Littlefield, Totowa, N.J.

Altman, I. (1975). *The Environment and Social Behavior*. Brooks/Cole Publishing Company, Monterey, California.

Banisar, D. (2002). *Freedom of Information: International Trends and National Security* Geneva.

Barkhuus, L. (2004). In *Privacy in Location-Based Services*, Concern v. Coolness. Paper presented at the Mobile HCI 2004 workshop: Location System Privacy and Control, Glasgow, UK.

Barkhuus, L. & Dey, A. (2003). *Location-Based Services for Mobile Telephony: a study of users' privacy concerns* (709-712). Paper presented at the Proceedings of Interact 2003, Zurich, Switzerland. ACM Press.

Belgian Linguistic Case (Application n° 1474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64) 23 July 1968, European Court of Human Rights judgment (see http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/)

Beresford, A. R. & Stajano, F. (2003). Location Privacy in Pervasive Computing. *IEEE Pervasive Computing*, *2(1)*, 46-55.

Bundesnetzagentur, 2007. *Jahresbericht* 2007.

Buruma, Y. (2001). *Buitengewone opsporingsmethoden* (2nd ed., Vol. 34). W.E.J. Tjeenk Willink, Deventer.

Cameron, I. (2000). *National security and the European Convention on Human Rights*.

Camp, L. J. & Osorio, C. (2002). *Privacy-Enhancing Technologies for Internet Commerce*. John F. Kennedy School of Government Harvard University Faculty Research Working Papers Series.

Chang, S. E., Hsieh, Y. J., Chen, C. W., Liao, C. K., & Wang, S. T. (2006). *Location-Based Services for Tourism Industry: An Empirical Study* (1144 - 1153). LNCS 4159. Springer-Verlag.

Clarke, R. (2001). *Person - Location and Person - Tracking: Technologies, Risks, and Policy Implications Information Technology & People*, *14(2)*, 206-231.

Colbert, M. (2001). A diary study of rendezvousing: implications for position-aware computing and communications for the general public (15-23). *Proceedings of Supporting Group Work, Boulder, Colorado,* USA. ACM Press.

Coliver, S. (1998). Commentary to: The Johannesburg Principles on National Security, Freedom of Expression and Access to Information. *Human Rights Quarterly*, *20(1)*, 12-80.

Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten, 2005. *Jaarverslag* 2004-2005

Cooley, T. M. (1880). *A Treatise on the Law of Torts, Or the Wrongs Which Arise Independent of Contract* (Cooley on Torts). Second Edition, *29*. Callaghan & Company, Chicago.

Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention no. 108)

Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms* (ECHR)

Court of Appeal in The Hague 25 January 2000 LJN AE0196, available at: http://www.rechtspraak.nl

Cvrcek, D., Marek Kumpost, Vashek Matyas, & Danezis, G. (2006). *A Study on The Value of Location Privacy*. a study undertaken in the framework activities around the FIDIS Network of Excellence presented at WPES 2006.

Danezis, G. Stephen Lewis, & Anderson, R. (2005). *How much is your privacy worth?* Fourth Workshop on the Economics of Information Security.

De Jong, J., Rietdijk, M. & Pluijmers, Y. (1997). Vastgoed persoonlijk benaderd. in: I. Van den Berg & A. Schmidt (Eds.), Samsom Bedrijfsinformatie bv, Alphen aan den Rijn/Diegem, 167-264.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal* L 281 , 23/11/1995 (1995).

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).

DPWP (Data Protection Working Party Article 29), 2005. Working document on data protection issues related to RFID technology.

DPWP (Data Protection Working Party Article 29), 2006. *CLOSING COMMUNIQUÉ*. Paper presented at the 28th International Conference of Data Protection and Privacy Commissioners.

Dudgeon: Dudgeon v. the United Kingdom, (application no. 7525/76), 22 October 1981, *European Court of Human Rights judgment* (see http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+ database/)

EC Regulations No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

EPIC (Electronic Privacy Information Center) & Privacy International, (2002). *Privacy and Human Rights 2002*; An International Survey of Privacy Laws and Developments.

Federal Constitutional Court, BVerfG, 1 BvR 2226/94 of 07/14/1999, Germany, available at: or http://www.bundesverfassungsgericht.de/ entscheidungen/rs19990714_1bvr222694en.html

Gavison, R. (1980). *Privacy and the Limits of Law*. The Yale Law Journal, 89(3), 421-471.

Gerards, J. (2006). Belangenafweging bij rechterlijke toetsing aan fundamentele rechten; Inaugural address as professor in Constitutional and administrative law.

GPS Case (2005), 25 BVerfG, 2 BvR 581/01 from April 12, Germany, available at http://www.bverfg.de/entscheidungen/rs20050412_ 2bvr058101.html.

Gruteser, M. & Grunwald, D. (2004). *A methodological assessment of location privacy risks in wireless hotspot networks*. Lecture notes in computer science, 2802, 10-24.

Hatton: Case of Hatton and Others v. UK (No.1), (application no. 36022/97 2003), 2 October 2001, *European Court of Human Rights judgment* (see http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+ database/)

Henrici, D. & Müller, P. (2004). Tackling Security and Privacy Issues in Radio Frequency Identification Devices. in: A. Ferscha & F. Mattern (Eds.), *PERVASIVE 2004*, LNCS 3001 Springer-Verlag Berlin Heidelberg, 219-224.

HR 21 March 2000 LJN AA5254, available at: http://www.rechtspraak.nl

HR 12 February 2002, Dutch Supreme Court, LJN AD9222, available at: http://www.rechtspraak.nl

HR 17 September 2002, Dutch Supreme Court, LJN AE4200, available at: http://www.rechtspraak.nl

HR 10 December 2002, Dutch Supreme Court, LJN AE9632, available at: http://www.rechtspraak.nl

HR 7 September 2004, Dutch Supreme Court, LJN AO9090, available at: http://www.rechtspraak.nl

Hunter v. Southam Inc., (1984) CanLII 33 (Federal Supreme Court of Canada; S.C.C.) http://www.canlii.org/en/ca/scc/doc/1984/1984canlii33/1984canlii33.html

IPTS (Institute for Prospective Technological Studies), (2003). *Security and privacy for the citizen in the post-September 11 digital age: A prospective overview*. Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home affairs (LIBE).

Jacoby, N. (2005). The Decision of the Bundesverfassungsgericht of April 12, 2005 – Concerning Police Use of Global Position Systems as a Surveillance Tool. The German Law Journal, 6(7), 1085-1092.

JupiterResearch. (2007). *Location-based services: where are you?* Cited by GPS Businessnews available at: http://www.gpsbusinessnews.com.

Kaasinen, E. (2005). User acceptance of location-aware mobile guides based on seven field studies. Behaviour & Information Technology, 24(1), 37-49.

Kamerstukken 1997-1998, nr. 25877. Parliamentary discussion Act on the Intelligence and Security Services 2002 (Behandeling van de WIV 2002) & Explanatory Memorandum Act on the Intelligence and Security Services 2002 25877(3).

Kamerstukken 1998-1999, 25403, nr. 25. *Parliamentary discussion Change of Code on Criminal Proceedings for special means for law enforcement* (Wijziging Wetboek van Strafvordering i.v.m. bijzondere opsporingsbevoegdheden) & Explanatory Memorandum (nr. 3)

Kamerstukken 2001–2002, nr. 28059(3). Explanatory Memorandum Change of Code on Criminal Proceedings to change mandates requisition telecommunication data (Wijz. van o.a. Wetboek van Strafvordering i.v.m. aanpassing bevoegdheden vorderen gegevens telecommunicatie).

Kamerstukken (2008). Niet-dossierstuk 30517 Tapstatistieken, verslag van een schriftelijk overleg, 23 September 2008

Klass: Klass and Others v. Germany, (application no. 5029/71), 6 September 1978, European Court of Human Rights judgment (see http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/)

Koops, B. J. (2006). *Tendensen in opsporing en technologie; Over twee honden en een kalf*. Wolf Legal Publishers, Nijmegen.

Koops, B. J. & Leenes, R. (2005). *'Code' and the Slow Erosion of Privacy. Michigan Telecommunications and Technology Law Review, 12(1)*, 115-188.

Krumm, J. (2007). In *A Survey of Computational Location Privacy*. Paper presented at the WORKSHOP ON UBICOMP PRIVACY, Innsbruck, Austria.

Leander: Leander v. Sweden (application no. 9248/81), 26 March 1987, European Court of Human Rights judgment (see http://www.echr. coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/)

Lee, G., Kim, W. & Kim, D. K. (2005). *An Effective Method for Location Privacy in Ubiquitous Computing*. LNCS (EUC Workshops 2005), 3823, 1006-1015.

Lemieux, D. (2007). *Privacy Impact Assessment from a Regulator's Point of View*. Paper presented at the Privacy Horizons: Terra Incognita (29th International Conference of Data Protection and Privacy Commissioners.

Levi, M. & Wall, D. S. (2004). Technologies, security, and privacy in the post-9/11 European information society. *Journal of Law and Society*, *31(2)*, 194-220.

Lockton, V., & Rosenberg, R. S. (2006). RFID: The next serious threat to privacy. *Ethics and Information Technology*, *7*, 221-231.

Longley, P. A., Goodchild, M. F., Maguire, D. J. & Rhind, D. W. (2001). *Geographic information Systems and Science*. John Wiley and Sons Ltd, Chicester, England.

Loof, J. P. (2005). *Mensenrechten en staatsveiligheid: verenigbare grootheden?* Wolf Legal Publishers, Nijmegen.

Luccio, M. (2006). *Skyhook Wireless Launches Wireless Position System*. GIS monitor,6 April.

Ludford, P. J., Frankowski, D., Reily, K., Wilms, K. & Terveen, L. (2006). Because I carry my cell phone anyway: functional location-based reminder applications (889 - 898). Paper presented at the Conference on Human Factors in Computing Systems*, Proceedings of the SIGCHI conference on Human factors in computing systems,* Montréal, Québec, Canada. ACM Press.

Marckx: Marckx v. Belgium, (application no. 6833/74), 13 June 1979, *European Court of Human Rights judgment* (see http://www.echr.coe.int/ ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/)

Margulis, S. T. (2003a). On the status and contributions of Westin's and Altman's theories of privacy. *Journal of Social Issues*, *59(2)*, 411-429.

Margulis, S. T., (2003b). Privacy as a social issue and a behavioral concept. *Journal of Social Issues*, *59(2)*, 243-261.

Marx, G. T., (1998). Ethics for the New Surveillance. *The Information Society*, *14*, 171-185.

Marx, G. T. (2002). What's new about the "new surveillance"? Classifying for change and continuity. *Surveillance and Society*, *1(1)*, 9-29.

McCullagh, D. (2006). *FBI taps cell phone mic as eavesdropping tool*. CNET News, December 4.

Mell, P. (1996). Seeking shade in a land of perpetual sunlight: privacy as property in the electronic wilderness. *Berkeley Technology Law Journal, 11*, 11-92.

Miedema, F. & Post, B. (2006). *Evaluatie pilot elektronische volgsystemen* Nijmegen.

Minister of Justice, (2008). Tapstatistieken, Brief aan de Voorzitter van de Tweede Kamer der Staten-Generaal, 27 mei.

Minister of Public Safety Canada. (2007). Annual report on the use of electronic surveillance 2006.

Mul, V., Verloop, P. C., Verbaan, J. H. J. & Bannier, M. C. (2005). Wie bewaart die heeft wat; Onderzoek naar nut en noodzaak van een bewaarverplichting voor historische verkeersgegevens van telecommunicatieverkeer.

Myjer, E. (2007). How can human rights best be guaranteed? in: Review Committee on the Intelligence and Security Services (CTIVD) & Faculty of Law Radboud University (Ed.), *Accountability of Intelligence and Security Agencies and Human Rights* (The Hague, 45-50.

Norris: Norris v. Ireland judgment, (application no. 10581/83), *European Court of Human Rights judgment* (see http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/)

Nouwt, S., de Vries, B. R. & Prins, C. (2004). *Reasonable Expectations of Privacy?* T. M. R. Asser Press.

O'Harrow Jr., R. (2005). *No place to hide; Behind the scenes of our emerging surveillance society*. The Free Press, New York.

Odell, M. (2005). *Use of mobile helped police keep tabs on suspect and brother*. Financial Times, August 2.

Olsson: Olsson v. Sweden (No.1), (application no. 10465/83), 24 March 1988, *European Court of Human Rights judgment* (see http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/)

Penders, J. (2004). Privacy in (mobile) telecommunications services. *Ethics and Information Technology*, *6*, 247-260.

R. v. Collins, (1987) 1 S.C.R. 265, Canada, available at: http://csc.lexum.umontreal.ca/en/1987/1987rcs1-265/1987rcs1-265.pdf

R. v. Duarte (1990) 1 S.C.R. 30, Canada, available at: http://scc.lexum.umontreal.ca/en/1990/1990rcs1-30/1990rcs1-30.pdf

R. v. Plant (1993) CanLII 70 (S.C.C.), Canada, available at: http://www.canlii.org/en/ca/scc/doc/1993/1993canlii70/1993canlii70.html

Rasterfahndung case (2006), 1 BvR 518/02 of 4 April 2006, Germany, available at: http://www.bverfg.de/entscheidungen/rs20060404_ 1bvr051802.html

Reiha, M. T. & Long, J. R. (2007). A 1.2 V reactive-feedback 3.1-10.6 GHz low-noise amplifier in 0.13 um CMOS. *IEEE journal of solid-state circuits*, *42(5)*, 1023-1033.

Reijne, Z., Kouwenberg, R. F. & Keizer, M. P. (1996). *Tappen in Nederland* (No. 90-387-0480-1). WODC/ Gouda Quint, Arnhem.

Roberts, A. (2002). Can we define terrorism? *Oxford today, 14(2)*.

Rotenberg, M., Laurant, C., Galster, U. & Rodríguez Pereda, K. (2006). 2006 *International Privacy Survey; An International Survey of Privacy Laws and Developments*. Electronic Privacy Information Center and Privacy International Washington D.C./ London.

Rotaru: Rotaru v. Romania, (application number 28341/95), 4 May 2000, *European Court of Human Rights judgment* (see http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/)

Rotenberg, M. & Knight, A. (2004). *Privacy and Human Rights 2004*. EPIC and Privacy International.

Rotterdamse politie, (2003). Het gebruik van (historische) verkeersgegevens in de opsporingspraktijk.

Schmid, G.T.C.E.-I., (2001). ONTWERPVERSLAG over het bestaan van een wereldwijd systeem voor de interceptie van particuliere en economische communicatie (ECHELON-interceptiesysteem).

Sietsma, R., (2007). Gegevensverwerking in het kader van de opsporing: toepassing van datamining ten behoeve van de opsporingstaak: afweging tussen het opsporingsbelang en het recht op privacy. Leiden University, Leiden.

Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights, Annex, UN Doc E/CN.4/1984/4 (1984). United Nations, Economic and Social Council, U.N. Sub-Commission on Prevention of Discrimination and Protection of Minorities(1984).

SIRC (Security Intelligence Review Committee), 2007. *SIRC Annual Report 2006-2007*; An operational review of the Canadian Security Intelligence Service.

Smith, J. & Kealy, A. (2003). SDI and Location Based Wireless Applications. in: I. Williamson, A. Rajabifard & M.-E.F. Feeney (Eds.), *Developing Spatial Data Infrastructures: From Concept to Reality* (Taylor and Francis, London, 263-279.

UN (United Nations) (2005). *The right of peoples to self-determination and its application to peoples under colonial or alien domination or foreign occupation, situation in occupied Palestine*, Report of the Secretary-General, UN Doc. E/CN.4/2005/13

US. v. Tomero (2006). SD New York, USA v. John Tomero Et Al., No. S2 06 Crim. 0008 (LAK)

US v. Forest (2004). 355 F.3d 942, 6th Circuit

van de Pol, W. (2006). *Onder de tap; afluisteren in Nederland*. Uitgeverij Balans, Amsterdam.

van Dijk, T. (2008). Nooit meer iets kwijt dankzij een zendertje. Delta 3.

van Loenen, B. & Zevenbergen, J. A. (2007). The impact of the European privacy regime on location technology development. *Journal of Location Based Services, 1(3)*, 165–178.

Veldkamp Marktonderzoek b.v. (2002). Nationaal Vrijheidsonderzoek; Een monitoronderzoek over 4 en 5 mei en achterliggende thema's (grondrechten, democratie, oorlog, vrijheid en verantwoordelijkheid). Nationaal Comité 4 en 5 mei.

Veldkamp Marktonderzoek b.v., (2003). Nationaal Vrijheidsonderzoek; Een monitoronderzoek over 4 en 5 mei en achterliggende thema's (grondrechten, democratie, oorlog, vrijheid en verantwoordelijkheid). Nationaal Comité 4 en 5 mei.

Veldkamp Marktonderzoek b.v., (2004). Nationaal Vrijheidsonderzoek; Een monitoronderzoek over 4 en 5 mei en achterliggende thema's (grondrechten, democratie, oorlog, vrijheid en verantwoordelijkheid). Nationaal Comité 4 en 5 mei.

Veldkamp Marktonderzoek b.v., (2005). Nationaal Vrijheidsonderzoek; Een monitoronderzoek over 4 en 5 mei en achterliggende thema's (grondrechten, democratie, oorlog, vrijheid en verantwoordelijkheid). Nationaal Comité 4 en 5 mei.

Venice commission (European commission for democracy through law), 2007. REPORT on the democratic OVERSIGHT of the security services (No. adopted by the Venice Commission at its 71s Plenary Session (Venice, 1-2 June 2007).

Verhue, D. (2007). Nationaal Vrijheidsonderzoek - opiniedeel meting 2007. Veldkamp, Amsterdam.

Verhue, D., Verzeijden, D. & Nienhuis, A. (2006). Nationaal Vrijheidsonderzoek; meting 2006; Een onderzoek naar opinie, kennis en draagvlak ten aanzien van 4 en 5 mei. Nationaal Comité 4 en 5 mei.

Walters, G. J. (2001). Privacy and security. *ACM SIGCAS Computers and Society, 31(2)*, 8-23.

Warren, S. D. & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, IV(5)*, 193-220.

Weber: Weber and Savaria v. Germany, (appl. no. 54934/00), 29 June 2006, *European Court of Human Rights judgment* (see http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/)

Westin, A. F. (1967). *Privacy and Freedom*. Atheneum, New York.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59(2)*, 431-453.

Wong, F. L. & Stajano, F. (2005). Location Privacy in Bluetooth. in: R. Molva, G. Tsudik & D. Westhoff (Eds.), *ESAS 2005, LNCS 3813*, 176-188.