Locating mobile devices

Balancing privacy and national security

Dr. ir. B. van Loenen
Prof. mr. J. de Jong
Mr. dr. ir. J.A. Zevenbergen

TU Delft

Onderzoeksinstituut OTB

Technische Universiteit Delft

This research has been funded by the Netherlands Organisation for Scientific Research (NWO) under grant number NVN 458-04-022

Authors:

Dr. ir. B. van Loenen
Prof. mr. J. de Jong
Mr. dr. ir. J.A. Zevenbergen

30 May 2008

OTB Research Institute for Housing,
Urban and Mobility Studies
Delft University of Technology
Jaffalaan 9, 2628 BX Delft, The Netherlands
Tel. +31 (0)15 278 30 05
Fax +31 (0)15 278 44 22
E-mail mailbox@otb.tudelft.nl
http://www.otb.tudelft.nl

Executive Summary

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 amongst these 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 commercial and government use of location information. 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 EU-Directive on privacy and electronic communications (2002/58/EC, OJ L 201) has anticipated this new ICT development. In addition to 'traffic data', necessary for the transmission of a communication, the directive uses the term 'location data', being the geographic position of the terminal equipment. Processing of any data for LBS is only allowed if the supplier has got prior, informed consent from the user. The user should have the possibility to block the processing of his location data (him being tracked) in an easy manner when he prefers so. Through the directive the EU has chosen for a strict OPT-IN regime including on-the-fly OPT-OUT.
However, the directive allows national legislation to override the EU provisions for a number of cases. For example, national laws can restrict the privacy protection when this is "a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system" (article 15). This poses the question to what extent government may collect and use tracking information to prevent terrorist attacks, or to satisfy other national security purposes, and consequently limit location privacy.
This research centralised around the question:

"How should the right to location privacy of users of mobile phones and other terminal equipment be balanced with the tracing and tracking interests of the (national) security sector?"

Research methodology
The research has been accomplished through a literature review on the concepts of privacy and national security. For both concepts, both literature from privacy and national security scholars have been studied as well as policy documents and court rulings. Special attention was provided to the rulings of the European Court of Human Rights concerning the balancing of privacy and national security interests. The aspect of location privacy and the role of location technology builds on a literature study which results were used as a basis for the interviews with several knowledgeable experts. The case studies on the Netherlands, Germany and Canada were performed through literature studies on the current legislation, court rulings on privacy and national security. Confirmation with the findings was sought through interviews which were partly accomplished through email communications.

Conclusions
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 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.

Contents

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 amongst these new ICT developments that potentially put the privacy of individuals at risk. LBS may be defined as geographically-oriented information services to users across mobile telecommunication networks (Karimi & Hammad 2004, p.350). 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 commercial and government 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 live. 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 EU-Directive on privacy and electronic communications (2002/58/EC, OJ L 201) has anticipated this new ICT development. In addition to 'traffic data', necessary for the transmission of a communication, the directive uses the term 'location data', being the geographic position of the terminal equipment. Processing of any data for LBS is only allowed if the supplier has got prior, informed consent from the user. The user should have the possibility to block the processing of his location data (him being tracked) in an easy manner when he prefers so. Through the directive the EU has chosen for a strict OPT-IN regime including on-the-fly OPT-OUT.
However, the directive allows national legislation to override the EU provisions for a number of cases. For example, national laws can restrict the privacy protection when this is "a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system" (article 15). This poses the question to what extent government may collect and use tracking information to prevent terrorist attacks, or to satisfy other national security purposes, and consequently limit location privacy.
This research centralised around the question:

"How should the right to location privacy of users of mobile phones and other terminal equipment be balanced with the tracing and tracking interests of the (national) security sector?"

1.1 Approach

The research report consists of three major components. First, since balancing the rights and limits to privacy is closely related to ethical and legal principles prevalent in a (western) society, the research explored core ethical and legal principles underlying the concept of privacy, and applies these principles to location privacy.
In addition, the research aimed to clarify the ambiguous concept of national security. A literature study together with examples from relevant national and international legislation and case law were used to provide information about situations where an appeal on national se-

curity may invade privacy in general, or location privacy more specific. Further, the research studied how the exemption of national security relates to other exemptions that may restrict privacy rights.

Finally, the research addresses the ambivalent role of technology. On the one hand technology may diminish location privacy and enhance national security through the possibility to trace and track mobile devices. On the other hand, technology also allows users to choose through privacy enhancing technologies not to be traced or tracked. The impact of technology on the balance between location privacy and national security will be studied, and the research will further address the implications the decision support model may have on technology or technological developments.
The outcomes of each of these aspects were used as the basis for the case studies.

1.2 Research scope

The general concept of privacy, national security and the feelings with regard to their balancing will be applied to the specific issue of location privacy, and more specifically to the tracing and tracking of mobile terminal devices by public authorities. In this respect, focus was on the tracking and tracing of mobile phones.
Personal data acquired from users of mobile devices is the focus of this study. More specific, the research objective is to address the acquisition of personal data through the real-time use of mobile equipment. Therefore, the research only addresses other personal data processes (not real-time) if this is relevant for the study.
Further, the main focus is on limiting the right to privacy for purposes of national security. National security is in this context combating serious crime and terrorism by (inter)national security and intelligence agencies. Other limitations such as law enforcement, disaster management, medical purposes were not the primary focus.
Also technical issues that concern data storage are not included in this study. The study does not research the impact on location privacy of the collection and use of location data for commercial purposes. Moreover, the research did not research the impact on location privacy on the collection and use of location data for commercial purposes.

1.3 Research methodology

The research methodology of this research is characterised as case study. Germany and Canada were selected since these are comparable to the Netherlands with respect to socio-economic development, but were assessed by Rothenberg et al. (through 2004-2006) to be countries with significant privacy safeguards in place. As opposed to the Netherlands which was assessed to have few privacy safeguards (Rothenberg et al. 2006).
The research has been accomplished through a literature review on the concepts of privacy and national security. For both concepts, both literature from privacy and national security scholars have been studied as well as policy documents and court rulings. Special attention was provided to the rulings of the European Court of Human Rights concerning the balancing of privacy and national security interests.
The aspect of location privacy and the role of location technology builds on a literature study which results were used as a basis for the interviews with several knowledgeable experts.
The case studies on the Netherlands, Germany and Canada were performed through literature studies on the current legislation, court rulings on privacy and national security. Confirmation with the findings was sought through interviews which were partly accomplished through email communications.

It should be noted that the research found resistance in the national intelligence and security agencies to cooperate. In the Netherlands, the national intelligence and security agency did not respond to requests for information, and the Review commission was unable to respond. In Germany, general questions about applicable law and the German legal system were answered, questions concerning the interpretation of the law and the operational activities of the intelligence service were considered to be too far reaching.
Based on these experiences, it was decided to dedicate for the Netherlands a separate case study to law enforcement, while for the other countries the scope was broadened to include case law that addressed law enforcement and privacy.

1.4 Reading guide

Chapter 2 addresses privacy. It will define privacy, look into the concepts, functions and perceptions of privacy in different contexts, and cultures. Finally, it will address location privacy. Chapter 3 provides an overview of international legislation on privacy and the underlying principles of these treaties, directives or guidelines. Chapter 4 lays down the issue of location information and its relation with privacy and national security. In chapter 5, national security is the focus. It explores internationally used definitions of national security, functions of protecting the national security and the need to use location information in protecting it. Chapter 6 addresses the technological means to protect or limit our privacy. Chapter 7 is the first chapter of the case-studies. In this chapter the situation concerning privacy and national security in the Netherlands will be analysed. For those interested in the balancing of privacy and law enforcement interests in the Netherlands are referred to chapter 8. The situation in Canada in balancing national security and privacy for mobile devices is discussed in chapter 9 and fro Germany in chapter 10. Chapter 11 brings together the theory on privacy, national security, and the findings from the case studies. In chapter 12 the conclusions of this research are presented.

2 Privacy

"You may not know about Acxiom, but it knows a lot about you"
(O'Harrow Jr. 2005, p.34)

In this chapter we will use a literature study on privacy to clarify the complex concept of privacy, its relation to other human rights and the speciality of location privacy. The literature study is based on a variety of sources with Westin (1967; 2003), Marx (1998), Raab and Bennett (1998), Walters (2001), IPTS (2003), and Margulis (2003) as the prominent literature.

2.1 Privacy defined

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. Others have described privacy as a vague catch-all phrase that includes a variety of concerns, such as respect for the personhood, dignity, and autonomy of the individual, private property, and solitude (Marx 1998, p.173).
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. As a consequence, the relationships between privacy and cognate concepts (e.g., deception, secrecy, anonymity) are debatable because the boundaries of the concepts are unclear and depending on specific circumstances (cf. Margulis 2003, 244). For example, where does privacy end and secrecy start?

Margulis (, 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 consequence, reduce vulnerability and increase decisional and behavioural options (Margulis , p.415). This, also, involves when personal information will be obtained and what uses will be made of it by others (, p.431). At a conceptual level, privacy may be defined as: "individuals their freedom of self-determination, their right to be different and their autonomy to engage in relationships, their freedom of choice, their autonomy as regards - for example - their sexuality, health, personality building, social appearance and behaviour, and so on" (IPTS 2003, p.139).
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).
A review of the definitions of privacy gives some insight in its meaning. A description of the functions of privacy and privacy rights, may increase the transparency of privacy as a concept.

Privacy stages
Four stages of privacy can be distinguished: (1) solitude, (2) intimacy, (3) anonymity, and (4) reserve (see Westin 1967). In the state of solitude the individual is separated from the group and freed from the observation of other persons (Margulis 2003, 412). It is the most complete state of privacy that individuals can achieve (see also Gavison 1980 cited by Mell 1996). In the state of intimacy a limited number of individuals exercises corporate seclusion so that

they may achieve an intimate, relaxed, and frank relationship (Westin 1967). Anonymity relates to be nameless in social interaction (Gavison 1980); the invisibility of individuals in public places, where he is free from identification and surveillance. In this state the individual is able to merge into the mass. Knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas (cf. Closed Circuit TV (CCTV) in public areas). Also anonymous relations and anonymous publication of ideas fall in the category. Finally, in a state of reserve a psychological barrier against unwanted intrusion is created; this occurs when the individual's need to limit communication about himself is protected by the willing discretion of those surrounding him (Westin 1967, p.31).

Four privacy stages:

- Solitude: to be free from observation by others;
- Intimacy: to be able to exercise corporate seclusion;
- Anonymity: to be free from identification and surveillance in public places;
- Reserve: to be able to limit communication about himself.

The importance of the four states is not necessarily equal. For example, research (see Westin 2003, 445 citing Harris Interactive and Westin 2001 and 1994) found that, in the US, citizens highly value intimacy (81% of US citizens values it as extremely important), where solitude (66%), reserve (55%) and anonymity (47%) were considered less important.

These general stages can also be applied to the current information society. In doing so, to be free from observation by others, incorporates no surveillance of modern communication means such as email, MSN, VoIP, digital TV, cell-phones (both conversation and location information), CCTV. Intimacy would require guaranteed peer-to-peer communication. Anonymity is the ability to use the Internet, and other modern technology without being recognized or identified. This will be extremely difficult since a defining characteristic of the information age is 'the disappearance of disappearance' (Haggerty et al. 2000, p.619), eliminating anonymity, in theory if not in practice. One may question whether this stage can ever be reached if one does not want to embrace the sort of primitive lifestyles enjoyed by the Unabomber and some extremist groups, since networked information technology effectively removes the right to seclusion from those who wish to participate in the information age (Levi and Wall 2004, p.206). Reserve specifically addresses communication and is in this context (almost) identical to intimacy.

2.2 The Right to Privacy: the limited access approach

The limited access approach is widely used to utilize the concept of privacy (see, for example, Westin 1967; Altman 1975; Gavison 1980; Mell 1996; Walters 2001; Camp and Osorio 2002; and Margulis 2003, 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/ 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.

Here, location information most often involved aspects of behavourial privacy. Bodily, and psychological privacy remain unaddressed in this study. Territorial privacy is only addressed if this appears to be relevant. This may be in instances of where the location of an event or behaviour takes place.

2.2.1 Privacy as a right to have freedom of movement

Privacy as a right to have freedom of movement may include both the concept of privacy as a right of autonomy and privacy as a right to seclusion; privacy as the degree of access to a person (including no access). The most basic autonomy right is the right to decide how to live one's life; the right to make choices and decisions (Feinberg 1986, p.54 cited by Lips et al. 2004, p.116). Autonomy implies that people are free if they and only they know where to go, when and how. The approach assumes that watched people are not free (see Buruma 2001, p. 33). The right to autonomy is interpreted rather absolute: no-one should know where one is, or what one is doing there. CCTV in public areas are unacceptable. The real-time location data from a cell-phone should not be used for tracing and tracking purposes.
Less far-reaching than autonomy is the view of privacy as a right to seclusion. Privacy as a right to seclusion refers to 'the right to be let alone' (Cooley 1880). Privacy in this respect is the ability to avoid unwanted contact and exposure of certain personal information (Camp and Osorio 2002, p.8). The critical element is the ability to refuse contact (Camp and Osorio 2002, p.9); the user of a device is in control. It is okay to be followed, but no interference please! Spontaneous happy birthday messages on the cell-phone from the service provider are not appreciated. The real-time location data from a cell-phone can be used for tracing

and tracking, but it is only accepted if it does not interfere with the activity of the individual. This approach assumes that knowledge that one may be tracked would not influence once behaviour (cf. Peissl 2002).

2.2.2 Informational privacy

Although the continuous tracking may not directly interfere with or influence one's behaviour or movements, the processed information can be stored, analyzed, and contribute to a profile of a user. As a consequence, the user may be confronted with unrequested special advertisements in the mailbox.

Informational privacy is the right to control information about oneself. The more information about an object is known, the better someone can utilize, manipulate or control this object. This applies to objects but also to people (ECP.NL 2005, p.16). A worst case example is the use of the Dutch population registration in the second world war by the Nazi's. The inclusion of one's religion in the registration was very useful to select those with Jew behind their names. If we manage to protect our personal information from the outside world, we will be more difficult to be influenced. In the information age, being able to control one's identity depends on the extent one's personal information has been provided to be included in a certain database. Informational privacy addresses the extent to which the individual is in control of the use of his personal information (Walters 2001, p.11; Westin 1967; Fried 1968; Rachels 1975; Lessig 1999). Warren and Brandeis (1890) addressed this aspect as follows:

> "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. Under our system of government, he can never be compelled to express them (except when upon the witness stand); and even if he has chosen to give them expression, he generally retains the power to fix the limits of the publicity which shall be given them. The existence of this right does not depend upon the particular method of expression adopted. It is immaterial whether it be by word or by signs, in painting, by sculpture, or in music. In every such case the individual is entitled to decide whether that which is his shall be given to the public."

Informational privacy has also been referred to as privacy as a property right (Raab and Bennett 1998, p.265). The individual has the control over his personal information and has the power to keep it confidential or to exploit it (IPTS 2003, 183). From this perspective privacy rights may be traded against other benefits for the individual. For example, one may allow the surveillance of his cell-phone in return for improved services based on a person's profile (Camp and Osorio 2002, p.9). Surveillance without any personal compensation would be unacceptable. Flaherty (1999) suggested the introduction of an information royalty system so that we are paid for the use of the commercial valuable personal data. In fact, this happens when people voluntarily trade personal information for tangible benefits, e.g., free email, bonus miles, discounts, or refunds (see Regan 2002; Mell 1996). A more questionable return may be national attention through 'voyeur television' (Westin 2003, 444) such as the Big Brother television show. The informational privacy right may also include the ability to masque one's real identity not to be bothered with not requested information such as direct mailing or spam (see Prins 2000, cf. Marx 1998). Prins (2006; see also Koops and Leenes 2005, p.186/7) criticizes the effectiveness of information as a property right approach: How to control the use of the personal data once it is out there? What to do with 'take it or leave it" contracts? What will be the administrative burden for paying for citizens' personal data?

2.2.3 Privacy of communications

Privacy of communications or relational privacy covers the security and privacy of mail, telephones, email and other forms of communication (cf. website GILC). It concerns the privacy of the content of the communication, i.e. the conversation. Issues like if, when, how, how often, and where a conversation takes place are not part of this right. This research centralises around the where question of mobile communication, however. Although relational privacy is irrelevant in this respect, legislation, jurisprudence, and privacy preferences or feelings puts location privacy at similar levels of importance as relational privacy. Therefore, this privacy right is addressed to the extent relevant.

2.3 Privacy functions

Privacy is a servant to many masters: it is not an end in itself, but merely a means to achieving other goals (Koops and Leenes 2005, p.134). These goals or functions may be individuality, autonomy, dignity, integrity, emotional release, self-evaluation, creativity, and limited and protected communication (Westin 1967, p.13; Pedersen 1999; Margulis 2003). Privacy allows for the development of individuality through protecting personal autonomy, supporting healthy functioning in society by "providing needed opportunities to relax, to be one's self, to emotionally vent, to escape from the stresses of life, to manage bodily and sexual functions, and to cope with loss, shock, and sorrow" (Westin 1967).

Privacy is important for the stimulation of personal relations because it allows for own choices to show your deepest personal thoughts and feelings. Without any bias or fear people may go further than they would otherwise and may arrive at more thoughtful, more creative and innovative solutions. Increased surveillance through, for example, databases with highly detailed personal information will have a 'chilling effect' on our willingness to deviate from the norm and on our willingness to question authority (Onsrud et al. 1994). Actions that are perceived negatively by the majority will be discouraged (Onsrud et al. 1994; Walters 2001, p.11). Privacy guarantees that each person is unique, and that one may act and think differently than the majority (IPTS 2003, 139).

In fact, one may argue that the increased transparency of individuals undermines the core values of democratic societies since it would substantially increase the likelihood of a "conformist, robotic public seeking to avoid exposure to the risks inherent in functioning in society" (Trubow 1990). The EU Article 29 Data Protection Working Party explains the impact privacy interferences may have on other functions or rights. They argue that the collection and use of vast amounts of personal information by public and private organisations leads to decisions, which directly influence peoples' lives. By classifying and profiling automatically or arbitrarily, these organisations can stigmatise in ways, which create risks for individuals and affect their access to services. They identified in such situations an increasing risk of social exclusion (DPWP, 2007). Privacy is an important guarantee to control these external powers on individuals because it ensures that these powers do not know everything about individuals and because it ensures that they do not judge citizens unfairly (Koops 2006, p.32). Without privacy others are deciding what choices you have in life (Koops 2006, p.32).

Examples in this respect are manifold. For example, house boat owners are not been served by a mail order company due to bad experiences with other house boat owners. Also financial institutions used redlining techniques making them decide to not provide mortgages to people that wanted to buy a house in statistically 'bad' neighborhouds (see, for example, Wishaw 2000, p.37). Similar profiling practices might block access to junk food, fast cars, dangerous sports, schools, energy supply or health care.

Article 29 Data Protection Working Party compared privacy with the air we breathe: "both are invisible, but when they are no longer available, the effects may be equally disastrous" (DPWP 2006, p.4).

2.4 Perceptions of privacy

The perception of privacy depends on a wide variety of aspects. Here we address the different privacy needs of people in identical contexts, the needs in relation to different contexts, the privacy needs as a cultural dependency, and address changing attitudes towards privacy within cultures, and contexts.

2.4.1 Privacy and people's needs

Privacy means different things to different people
(Westin 2003, p.445)

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, 442). Some people love to give away their full personal life in TV shows, while others are very reserved in providing their phone number or address. Westin (2003, p.445, citing Louis Harris & Associates & Westin 1995) found three ideological-interest positions on privacy:

- privacy fundamentalists;
- privacy pragmatists, and
- privacy unconcerned.

These ideological-interest positions on privacy may well compare with the positions on privacy as a social issue. Margulis (2003, p.250; see also Westin 2003, p.434) identified the high, balanced and limited privacy position.
Typically, those taking the high-privacy position are the privacy aware; having unlisted phone numbers, using proxy servers on the internet and frequently using one of Marx' behavioural techniques (Marx 1998) to maximize the level of privacy. Their perceptions of privacy are close to privacy as a right of autonomy. The privacy pragmatists, or the balanced view may be close to the 'right to seclusion' perception; privacy is valued but certain government interventions are accepted. The privacy unconcerned, or the limited privacy position, may be associated with those that perceive privacy as a property right. They assign a lower value to privacy claims than to business efficiency and societal-protection interests and it opposes governmental intervention to protect privacy as unnecessary and costly (Margulis 2003, 250). Grossklags and Acquisti (2007) refer to Taylor (2003) suggesting that most people are privacy pragmatists since they are willing to trade off personal information for other benefits.
Privacy concerns, however, do not necessarily equal privacy behaviour. In an analysis of research addressing privacy concerns of internet users, Van der Geest et al. (2005, p.5) found that almost everybody is concerned about being tracked across websites, while only 10% uses available software to prevent the installation of cookies on their computer. Further, users with strong privacy concerns readily disclosed sensitive personal data on websites (Spiekermann et al., 2001, p.43). Spiekermann et al. conclude that people express their desire to be in control, but when given the opportunity, they do not use it (see also Grossklags and Acquisti 2007). One may wonder to what extent people oversee the consequences of disclosing their personal data to organisations they may not trust, or consenting to privacy intrusive contracts

of which they did not know about content of boilerplate licenses (see also Van der Geest et al. 2005). Adding this to the willingness of selling personal information for a small treat, one may wonder how people really conceive the theoretical loss of privacy (see also Koops and Leenes 2005, p.184).

2.4.2 Privacy and context

Privacy conceptions are different in different contexts

The attitude of individuals towards their privacy is context-depending. Raab and Bennett (1998, p.267) explain this nicely as follows:

> "[] in daily life, the individual moves through sectoral contexts with different privacy configurations and may have varying attitudes toward these. She tells her doctor what she does not tell her bank. Her tutor does not have to know her financial details, but she cannot withhold these from the tax office. She does not want the benefits office to give her information to her landlord, but would not mind if her solicitor knows her shareholdings. She is more afraid of what her insurance company does with her personal data than what the driving-license bureau does. She thinks that her privacy is more at risk from direct marketers than from her pension fund. She enjoys the convenience of booking theatre tickets by telephone with her credit card. Where possible, she may adopt selective strategies for controlling who knows what about herself, and her propensity to raise complaints may vary. She is unaware of many things that are being done 'out there' with her data, and worries about some of the possibilities. But she is comfortable with the trade-offs that she makes and the risks that she believes she runs".

Similarly, contexts may change and impact attitudes towards privacy (see Westin 1967, 2003, 433; Margulis 2003). 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 exchange and in certain instances one expects that data is exchanged; e.g., the doctor exchanges your personal file with the hospital. However, we would object against exchanging personal data between spheres. For example, your doctor exchanging your medical file with your health insurance company.

2.4.3 Privacy and culture

What must be kept private seems to differ from society to society (Whitman 2004, p.1153). It has been suggested that the privacy perception depends on cultural aspects (Bellman et al. 2004, p.322). Whitman (2004) provides supportive arguments when he explains the differences in the perception of privacy in continental Europe and the United States. He quotes a German internet site saying that it is normal in the US "for a host at dinner to ask "not just how much you earn, but even what your net worth is" – topics ordinarily quite off-limit under the rules of European etiquette" (Whitman 2004, p.1155-1156). A European would also have difficulty to understand the justification of the disclosure of intimate details in the Monica Lewinsky investigation (Whitman 2004, p.1155). On the contrary, Americans do not understand privacy in (European) countries where "people prance around naked out of doors while allowing the state to keep tabs on their whereabouts, convict them on the basis of unfair police investigations, peer into their living rooms, tap their phones, and even dictate what names they can give to their babies" (Whitman 2004, p.1159). Another example show-

ing the cultural differences is the news the Australian newspaper Herald brought. They found in the Netherlands several sunbathers nude on imagery provided by GoogleEarth "in a distance not far from the Dutch parliament" (Hutcheon 2006). In the Netherlands, the issue never made it to the news.
Countries that perceive privacy differently (see Whitman 2004, p.1159) may address the right to privacy also differently in, for example, legislation. It has been argued that continental etiquette is overwhelmingly about 'the presentation of self in everyday life', just like continental privacy law" (emphases on one's dignity: Whitman 2004, p.1168). In the U.S. the core privacy right is the right to freedom from intrusions by the state, especially in one's own home (emphases on one's liberty: Whitman 2004, p.1161). Although Americans and Europeans do sometimes arrive at the same conclusions, he argues, they have different starting points and different ultimate understanding of what counts as a just society (Whitman 2004, p.1163). As a result there are two different cultures of privacy, which are home to different intuitive sensibilities, and which have produced two significantly different laws of privacy (Whitman 2004, p.1160).

Europeans trust government more than the private sector with personal information (Whitman 2004, p.1193). This may explain why government in Europe quietly can tap people's telephones: in Europe compared to the US and other Anglo-Saxon countries a suggested rate of thirty times more taps are placed in Germany and 130 times more in the Netherlands (see Albrecht et al. 2003, p.7). It may further explain why in the U.S. law enforcement and national security agencies need a court order to tap a phone, while in the Netherlands consent of the responsible Magistrate (*Rechter-commissaris*) is also required for law enforcement taps, but only consent of the Minister for national security purposes.

In some cultures men have no physical defence against the outside world. The result is that their defences are mostly psychological (e.g., hide their feelings, emotional restraint, a lack of candour in both speech and behaviour (Westin 1967, p.16). Similarly, the use of Closed Circuit TV can be considered in one country as a way to protect public safety, while in another as infringing the right to privacy. In this respect, it has been argued that what is important is not what the technology does, but rather how it fits into cultural practice (Palen et al. 2003).

2.4.4 Changing attitudes towards privacy

Privacy is a living, continuously changing thing dependent on socio-cultural factors (Koops and Leenes 2005, p.132). We regulate privacy so it is sufficient for serving momentary needs and role requirement) (see Margulis 2003 referring to Westin 1967). At least five factors drive privacy concerns (Margulis 2003, 250; Westin 2003; Koops and Leenes 2005, p.133):

1. new technologies and their uses by government and businesses;
2. social climate and public attitudes;
3. interest group activities and policy debates;
4. organizational policies and legislation, and
5. the fading importance of national boundaries.

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 localization is becoming an increasingly common side-effect of technology."

They further note especially in the context of privacy a considerable lack of awareness among the general public of the potential (mis)uses of technologies: they can and will be used against you (Koops and Leenes 2005, p.181; see also O'Harrow 2005).

2.5 Conclusion

Privacy exists and performs in many shapes and sizes. Although some, mostly privacy scholars, warn for the impact of the loss of privacy, many regular citizens ignore these warnings, either because they are ignorant, unaware, or unable to oversee the consequences of the loss of something that remains a vague concept and which does not need to protect those that have nothing to hide.

This chapter has primarily built on privacy literature exploring the concept of privacy, aiming to make it a concept more easy to capture. It has explained the critical function privacy may have in society, and more theoretically its definition, explained its different stages, the different privacy rights, and privacy perceptions, including changing attitudes towards privacy. Despite the difficulties to establish exact boundaries around privacy several conclusions can be drawn from the literature review.

In western societies, the limited access approach is commonly used as a concept to capture privacy. This approach emphasizes the autonomous individual, choice and control, and social relationships as voluntary or as barriers to independence. The control over access to self and over the information about someone are central. The extent to which individual's privacy needs are satisfied depends on a variety of factors: the context, culture and the individual's perception of privacy.

In following chapter we will see how the right to privacy is embedded in international treaties and legislation and how privacy has been balanced with other interests of society. We will then in chapter 4 focus on location privacy.

3 Privacy as a fundamental human right

Privacy is a fundamental human right as being recognized by international law such as the United Nations' International Bill of Human Rights and the (European) Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe (ECHR). In addition, specific international and national legislation has been developed to protect the privacy of individuals in the processing of their personal information. The rules of the Organisation for Economic Co-operation and Development (OECD) for data protection and Convention nr 108 of the Council of Europe are examples of such legislation.
In this chapter, we analyse the body of international legislation most relevant for this study. We analyse the general privacy principles underlying the treaties, conventions, opinions, guidelines, and rulings of the European Court of Human Rights (EctHR). Focus is both on privacy as a human right and privacy with respect to personal data protection.

3.1 United Nations

The United Nations' International Bill of Human Rights consists of the Universal Declaration of Human Rights, the International Covenant on Economic, Social and Cultural Rights, and the International Covenant on Civil and Political Rights (ICCPR) and its two Optional Protocols. Privacy is addressed in the Universal Declaration of Human Rights (article 12), and the ICCPR (article 17)[1]. They were further developed by the UN Economic and Social Council in the Siracusa principles.

3.1.1 Universal Declaration of Human Rights (1948)

Article 12 of the Universal Declaration of Human Rights reads:[2]

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

The Universal Declaration of Human Rights contains a general provision applicable to all the rights provided for in the Declaration authorizing restrictions on their exercise. It affirms that the exercise of a person's rights and freedoms may be subject to certain limitations, which must be determined by law, solely for the purpose of securing due recognition of the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society. Thus, certain safeguards provided, national security may be a cause to limit the right to privacy. It does not distinct or put an order between different human rights. The Declaration does not contain a special enforcement regime.

3.1.2 International Covenant on Civil and Political Rights (1976)

The International Covenant on Civil and Political Rights (ICCPR) addresses privacy in its' article 17:

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

[1] Website OHCHR 2

[2] Adopted by the United Nations in 1948.

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

The ICCPR distinct three types of human rights[3]:

- absolute human rights: rights that never may be suspended or limited, even in emergency situations[4];
- normal rights: rights which may be limited or suspended in cases of officially proclaimed public emergencies, which threaten the life of the nation;
- restrictable rights: rights which shall not be subject to any restrictions except those which are prescribed by law and are necessary to protect national security, public order, or the rights and freedoms of others.[5]
  (website OHCHR)

Privacy, i.e. the prohibition of arbitrary or unlawful interference with an individual's privacy, family, home or correspondence, and of unlawful attacks on his honour and reputation (art. 17), is a normal right under the ICCPR.

A special Human Rights Committee monitors the implementation of the ICCPR by its state's parties. The Committee may consider inter-state complaints and States must report whenever the Committee requests (usually every four years). The Committee examines each report and addresses its concerns and recommendations to the State party in the form of "concluding observations" (website OHCHR).
The Human Rights Committee has addressed the issue of surveillance measures in General Comment 16, §8: "Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited" (see website University of Minnesota). Despite this strict language, the concluding comments to various State reports make it clear that surveillance measures are permissible when strictly controlled and overseen by independent, preferably judicial, bodies (Zöller 2004, p. 482 referring to Concluding Comments on Poland, UN doc. CCPR/C/79/Add. 110 (1999); Concluding Comments on Zimbabwe, UN doc. CCPR/C/79/Add. 89 (1998); Concluding Comments on Lesotho, UN doc. CCPR/C/79/Add. 106, 24 (1999)).

3.1.3 Siracusa principles (1984)

The Siracusa principles are the result of a meeting of 31 experts in international law. They met in Siracusa, Sicily, in 1984 to consider the limitation and derogation provisions of the ICCPR.
They agreed that in time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, countries may take measures derogating from the obligations of the Covenant (article 4.1 Covenant). The right to privacy is one of the rights which can only be derogated from in a stage of emergency.

[3] The International Covenant on Civil and Political Rights (1966) entry into force 23 March 1976. The Covenants, by their nature as multilateral conventions, are legally binding only on those States, which have accepted them by ratification or accession. [] Judges of the International Court of Justice have occasionally invoked principles contained in the International Bill of Human Rights as a basis for their decisions (website OHCHR 3).
[4] Loof (2005, 188), however, argues that in a state of emergency none of the fundamental rights are absolute: not all circumstances justify that fundamental rights should prevail over other interests of the community.
[5] These typically include a phrase like "No restrictions may be placed on the exercise of this right other than those imposed in conformity with the law and which are necessary in a democratic society in the interests of national security or public safety, public order (*ordre public*), the protection of public health or morals or the protection of the rights and freedoms of others."

The Siracusa Principles on the Limitation and Derogation of Provisions in the ICCPR[6] further developed the ICCPR. They stress that (article 10):
"Whenever a limitation is required in the terms of the Covenant to be "necessary," this term implies that the limitation:

(a) is based on one of the grounds justifying limitations recognized by the relevant article of the Covenant,
(b) responds to a pressing public or social need,
(c) pursues a legitimate aim, and
(d) is proportionate to that aim.

Any assessment as to the necessity of a limitation shall be made on objective considerations."

3.1.4 Summary of United Nations privacy principles

The United Nations has developed general principles on the right to privacy. Privacy is addressed in the Universal Declaration of Human Rights (article 12), and the ICCPR (article 17). It can be assessed to be a right that can only be derogated from in time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed. In a time of emergency the right to privacy can be limited only if the limitation is necessary and assessed on objective considerations and proportionate to the aim of overcoming the public emergency. Surveillance is permitted only when strictly controlled and overseen by independent bodies.

3.2 OECD principles for personal data processing (1981)

Within the United Nations' framework privacy as a human right is recognized. The framework has not further developed the right, for example, for personal data protection. For the use of personal data in computerized systems, the Organisation for Economic Co-operation and Development (OECD) developed specific guidelines, which would help to harmonise national privacy legislation and, would prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it. The Guidelines, in the form of a Recommendation by the Council of the OECD, were adopted and became applicable in 1980 (preface of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data). In 1998, the OECD Ministers recognised that the 1980 Privacy Guidelines were still applicable in that they 'represent international consensus and guidance concerning the collection and handling of personal data in any medium, and provide a foundation for privacy protection on global networks' (OECD Ministerial Declaration on Privacy on Global Networks 1998 (website OECD Ottawa)).

[6] United Nations, Economic and Social Council, U.N. Sub-Commission on Prevention of Discrimination and Protection of Minorities

The OECD guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties (article 2 OECD).

The eight basic principles are:

1. the collection limitation principle; There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject (article 7 OECD).

2. the data quality principle; Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date (article 8 OECD).

3. the purpose specification principle; The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose (article 9 OECD).

4. the use limitation principle; Personal data should not be disclosed, made available or otherwise used for specified purposes other than those specified in accordance with principle 9 of the OECD (see above) except: a) with the consent of the data subject; or b) by the authority of law (article 10 OECD).

5. the security safeguards principle; Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data. (article 11 OECD)

6. the openness principle; There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller. (article 12 OECD)

7. the individual participation principle; An individual should have the right:
    a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
    b) to have communicated to him, data relating to him:
        1. within a reasonable time;
        2. at a charge, if any, that is not excessive;
        3. in a reasonable manner; and
        4. in a form that is readily intelligible to him;
    c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
    d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended. (article 13 OECD)

8. the accountability principle; A data controller should be accountable for complying with measures which give effect to the principles stated above. (article 14 OECD)

Exceptions to the Principles include those relating to national sovereignty, national security and public policy. These restrictions should be: a) as few as possible, and b) made known to the public (article 4 OECD).

The OECD guidelines have been used as the starting point in the development of international legislation concerning personal data processing in OECD member countries.

3.3 Council of Europe privacy principles

The Council of Europe seeks to develop throughout Europe common and democratic principles based on the (European) Convention for the Protection of Human Rights and Fundamental Freedoms (further ECHR) and other reference texts on the protection of individuals (website Council of Europe). It requires contracting parties to implement the principles set forth by the Convention. It has 47 European countries as member, and one applicant country (Belarus).
The ECHR, article 8, provides the general legal basis for the right to privacy. Article 8 reads:

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 Council of Europe detailed the right to privacy specifically for personal data processing through the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention no. 108). The Committee of Ministers has adopted in 2002 the ”Guidelines on human rights and the fight against terrorism”. Also they are included in this section.

3.3.1 Convention for the Protection of Human Rights and Fundamental Freedoms

Similar to the United Nations' legislation, the ECHR also distinguishes absolute, normal and restrictable rights (IPTS 2003, 141). The Convention recognizes that absolute rights must be respected even when in times of emergency when derogations to other rights are justified (art. 15(2)). Absolute human rights are the right to life (art. 2), prohibition of torture (art. 3), prohibition of slavery (art. 4(1)), and no punishment without law (art. 7). Normal rights are rights, which can be derogated from, only in times of emergency (art. 15(1)). These are the right to liberty and security (art. 5), the right to a fair trial (art. 6). Finally, the Convention recognizes rights, which can be legitimately restricted in terms of emergency but also under some specified conditions (IPTS 2003, 141). These are the right to respect for private and family life (art. 8), freedom of thought, conscience and religion (art. 9), freedom of expression (art. 10), and the freedom of assembly and association (art. 11).
Where the UN places the right to privacy as a normal right (i.e. only restrictable if the life of the nation is threatened), the ECHR categorizes it as a less absolute human right. Therefore, it can be argued that at the European level, privacy is a relatively weak fundamental right (IPTS 2003, 141). In addition, the UN absolute right of freedom of thought, conscience and religion is in the European context only a restrictable right. The implications of these differences are unclear.

Human right	UN	EU
Rights to life	A	A
Freedom from torture	A	A
Freedom from slavery	A	A
Protection from imprisonment for debt	A	-
Freedom from retroactive penal laws	A	A
Right to recognition as a person before the law	A	-
Freedom of thought, conscience and religion	A	R
Right not to be subjected to arbitrary arrest or detention	N	N
Right that all persons deprived of their liberty are to be treated with humanity	N	N
The equality of all persons before the courts and tribunals and for guarantees in criminal and civil proceedings	N	N
The prohibition of arbitrary or unlawful interference with an individual's privacy, family, home or correspondence, and of unlawful attacks on his honour and reputation	N	R
The enjoyment of the highest attainable standard of physical and mental health	R	-
Freedom of opinion and expression	R	R
Right of peaceful assembly	R	R
Right to freedom of association	R	R

Table 3.1: Categorization of human rights by UN and EU compared

(A= absolute right; N= normal right; R= restrictable right)

3.3.2 European Personal Data Processing Protection: Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention no. 108)

This Convention is the result of the process dating back to 1968 when the ECHR and domestic law were assessed to offer inadequate protection to the right of personal privacy with regard to 'modern society and technology' (see Explanatory report Convention 108).
Convention 108 may be regarded as an extension of the ECHR. It should result in a harmonisation of the laws of the contracting states and hence decrease the possibility of conflicts of law or jurisdiction (Explanatory report).
In 1980, it was decided not to incorporate a provision on the protection of personal data in the ECHR. Instead, it provides clear and precise indications on the purpose to be achieved by each principle, but leaves to each country, the manner of implementing it in its domestic law (Explanatory report). The Convention was not designed to be self-executing with the result that individual rights cannot be derived from it. Further, the Explanatory report reads that it should be left to each State to determine the nature of sanctions and remedies (civil, administrative, criminal).
The purpose of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) is to secure respect for every individual's rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him (see art. 1 Convention 108). The focus is on the processing of personal data. Article 5 of Convention 108 provides the general principles for data processing (the 'common core').

"Personal data undergoing automatic processing shall be:

a. obtained and processed fairly and lawfully;
b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
d. accurate and, where necessary, kept up to date;
e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored"

Further, article 7 rules that appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination. Article 8 provides the data subject rights to establish the existence of an automated personal data file, the right to rectify personal data, and to have a remedy if his request is not complied with.

Convention 108 allows for derogation from the 'privacy principles' when such derogation is provided for by the national law and constitutes a necessary measure in a democratic society in the interests of: protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences, and protecting the data subject or the rights and freedoms of others (art. 9(2) Convention 108).

Convention 108 has been assessed to be rather unimportant and not very influential with regard to the right to private life of Article 8 ECHR: "[..] the Strasbourg Court and Commission have paid very little attention to 'their own' Council of Europe's Treaty 108" (IPTS 2003, 123). Exception may be the judgment in *Rotaru* in which the European Court of Human Rights used the Convention 108's broad interpretation of personal data in its decision whether the case involved personal data.

3.3.3 Guidelines on human rights and the fight against terrorism

In the Guidelines on human rights and the fight against terrorism adopted by the European Committee of Ministers in 2002 (EU 2002) privacy and the fight against terrorism are addressed in articles V and VI. Article V requires appropriate provisions of domestic law, proportionality to the aim for which the collection and the processing were foreseen, and allows for supervision by an external independent authority. In article VI it is explicitly stated that it must be possible to challenge before a court the lawfulness of measures used in the fight against terrorism that interfere with privacy.

3.4 European Court of Human Rights

The European Court of Human Rights (ECtHR) is the authority that rules on the extent to which the right to privacy may be intruded for purposes of national security, among others. It oversees the implementation of the ECHR. The contracting countries undertake to abide by the final judgment of the ECtHR in any case to which they are parties (art. 46(1) ECHR). The final judgment of the ECtHR shall be transmitted to the Committee of Ministers, which shall supervise its execution (art. 46(2) ECHR).

The ECtHR's rulings on article 8 ECHR have developed a rather solid framework further specifying and explaining article 8. Data protection and privacy issues or aspects can also be found in the Articles 5, 6, 10 and 13 ECHR. In this section we evaluate several key judg-

ments that provide the framework for balancing privacy with national security interests. In its' rulings, the ECtHR has developed upon the requirements that an intrusion of the right of privacy should be 'in accordance with the law' and 'necessary in a democratic society' (see article 8.2 of the Convention). Building on the ECtHR's judgments, this section summarises how article 8.2 should be interpreted. 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.

3.4.1 ECtHR's interpretation of the concept of privacy

In his assessment of ECtHR rulings on privacy, Buruma (2001) noted the following key judgments on the ECtHR's interpretation of privacy. The ECtHR has stated that the essential object of article 8 is to protect the individual against arbitrary action by the public authorities (*Kroon*).
In *Niemietz* the ECtHR further stressed that "it would be too restrictive to limit the notion (of private life) to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude there from entirely the outside would not encompassed within that circle".
In addition, a reasonable expectation of privacy may be of interest (see *Halford*). Although this was later indicated to be only one of the criteria to be used in an assessment of privacy infringement (see *P.G. and J.H.*). In *Luedi*, the ECtHR stated that a person involved in criminal activities is entitled to a lesser expectation of privacy. Concerning phone calls at work, the ECtHR ruled that employees have a reasonable expectation of privacy when making phone calls. An employer monitoring phone calls was an interference with article 8 ECHR (*Halford*).

3.4.2 Private and family life, home and correspondence (communications)

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).
In *Peck* the ECtHR reiterated that elements such as gender identification, name, sexual orientation and sexual life are protected by Article 8. Article 8 also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature. The ECtHR identifies a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life' (*Peck*).
The ECtHR has also addressed the extent to which phone calls fall within the scope of article 8. The ECtHR holds that "tapping and other forms of interception of telephone conversations constitute a serious interference with private life" (*Kopp* §72). Telephone calls made from business premises as well as from the home may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8.1 (see *Klass*; *Malone* § 64; *Huvig*; *Niemietz* §§ 29-33; *Halford* §44). In *Weber*, the ECtHR also hold the ubiquitous monitoring of satellite telephone conversations as an interference of article 8. Thus, (cell) phone conversations are within the scope of article 8. But is this also applicable to the location of the (cell) phone? The ECtHR has not (yet) addressed this aspect.
It has distinguished between measures effected outside a person's home or private premises and measures effected in public spaces. The ECtHR ruled that walking in public areas such

as a street implies that one is visible to any member of the public present in that same space. The ECtHR considers the monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) of a similar character. However, once any systematic or permanent record comes into existence of such material from the public domain, private life considerations may arise (*P.G. and J.H.* § 57).
In the context of photographic equipment recording the visual data, the systematic monitoring of a specific individual in public space gave rise to an interference with the individual's private life (see, for example, *Herbecq* § 92).
In both *Rotaru* and *Amann* the compilation of data by security services on particular individuals (even without the use of covert surveillance methods) constituted an interference with the applicants' private lives (*Rotaru* §§ 43-44, and *Amann* §§ 65-67).

Based on the above, it is most likely that there are instances where the tracing and tracking of location information of the cell-phone can be considered as an interference with article 8. In judging whether there is a privacy interference, the location (public or private space), the duration and way (systematic or not) of the processing manners. Also what one is doing in public space (participating in a public event), being a public figure, or whether one is charged with or convicted of an offence may be relevant.

3.4.3 When is interference justified?

When is interference with the private life and communications justified? Article 8(2) of the ECHR provides the basis for the ECtHR's rulings. The ECtHR's judgments take into account whether:

- the interference is in accordance with the law, and
- the interference is necessary in a democratic society.

Where the ECtHR finds a measure is not 'in accordance with the law' it does not proceed to assess whether the requirements of 'necessary in a democratic society' are being adhered to.

3.4.3.1 Whether an interference is 'in accordance with the law'

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).

In accordance with the law

1. Impugned measure has some basis in domestic law
2. The law is accessible to the person concerned
3. The law is foreseeable as to its effects to the person concerned
4. The law is compatible with the rule of law: it provides effective remedies (both in practice as in law) against arbitrary interference by public authorities:
    - authority carrying out the control needs to be sufficiently independent (preferably with representatives of parliament including the opposition), and
    - vested with sufficient powers and competence to exercise an effective and continuous control

Accessibility

The law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case (*Sunday Times* §49; *Silver* §§87-88).

Foreseeability

The consequences of the law must be foreseeable for the individual concerned (see Malone, § 67). Thus, 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[7] (see *Malone* § 67; *Leander* §§ 50-51; *Kahn* 2000, § 27; *Halford* 1997, § 49).

The requirement of foreseeability in the special context of national security, cannot be the same as in many other contexts. "The requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly" (*Malone* § 67; *Leander* § 51). In specific instances it is appropriate to not inform individuals about the existence of personal data within national security and intelligence agencies. "On this point, the Court, [], recalls the necessarily limited effectiveness that can be required of any remedy available to the individual concerned in a system of secret security checks" (*Leander* § 82).

Principle: 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.

The law is compatible with the rule of law

The ECtHR has ruled that interference can only be regarded as 'in accordance with the law' if the particular system of secret surveillance adopted contains effective and adequate guarantees against abuse (*Malone* §§ 49-50; *Klass* §§ 49-50; *Leander* §60). This is because of the inherent secrecy of the exercise of such secret powers which carry with them a danger of abuse

[7] ""Domestic law" may be taken in a wide sense, i.e. not only legislation but also appropriate or specific regulations or administrative directives, as long as the necessary level of protection is secured" (Explanatory report Convention 108; see also *Leander* §51).

of a kind that is potentially easy in individual cases and could have harmful consequences for democratic society as a whole (*Malone* §56).
Interference with an individual's rights should be subject to an effective control, especially when the interferences involve secret surveillance by intelligence services. This should normally be assured by the judiciary, at least in the last resort, since judicial control offers the best guarantees of independence, impartiality and a proper procedure (*Klass* §§55-56; *Segerstedt* §76; *Leander* §50; *Malone* §67). The independent 'authority' may not necessarily in all instances be a judicial authority. But the powers and procedural guarantees the authority possesses are relevant in determining whether the remedy is effective (*Rotaru* §69; *Segerstedt* §117). Furthermore, where secret surveillance is concerned, objective supervision may be sufficient as long as the measures remain secret. It is only once the measures have been divulged that legal remedies must become available to the individual (*Rotaru* §69; *Segerstedt* §117; *Weber* §135; *Klass* §58; *Leander* §66).
In *Leander*, a controlling authority lacking the power to render a legally binding decision, and which only exercises general supervision and does not have specific responsibility for inquiries into secret surveillance or into the entry and storage of information on the Secret Police register were not considered by the ECtHR to be effective within the meaning of Article 13 of the Convention (*Segerstedt* § 118).

In *Klass,* the ECtHR provides guidelines for adequate measures against abuse:

> "Review of surveillance may intervene at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding the individual's rights."

The assessment of adequate and effective guarantees against abuse has only a relative character: "it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law" (*Klass*; see also *Weber* §106; Kamerstukken 22036 nr. 6).

Adequate safeguards for secret phone tapping
In a recent case, the ECtHR found the German remedy for ubiquitous monitoring of satellite telephone conversations effective (*Weber* §152-156). The Federal Minister is empowered to decide on the use of intrusive means by the Federal or state prime minister. The independent parliamentary Supervisory Board, consisting of members of parliament, including members of the opposition needs to be informed at least every six months about the implementation of the law. Further, the independent Supervisory Commission has to authorize surveillance measures and has substantial power in relation to all stages of interception (*Weber* §§117,24; cf. *Segerstedt* §118). Moreover, monitoring needs to be discontinued immediately once the conditions set out in the monitoring order are no longer fulfilled or the measures themselves are no longer necessary (*Weber* §116).
In *Weber*, the ECtHR acknowledges that it is essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated (*Weber* referring to *Kopp* §72, and *Valenzuela Contreras* §46).

In its case-law on secret measures of surveillance, the ECtHR has developed the following minimum safeguards that should be set out in statute law to avoid abuses of power:

- the nature of the offences which may give rise to an interception order;
- a definition of the categories of people liable to have their telephones tapped;
- a limit on the duration of telephone tapping;
- the procedure to be followed for examining;
- using and storing the data obtained;
- the precautions to be taken when communicating the data to other parties; and
- the circumstances in which recordings may or must be erased or the tapes destroyed

(*Weber* §95; *Huvig* §34; *Amann* §76; *Valenzuela Contreras* §46; and *Prado Bugallo* §30).

We may conclude that effective remedy requires that the authority carrying out the control needs to be sufficiently independent (preferably with representatives of parliament including the opposition), and vested with sufficient powers and competence to exercise an effective and continuous control (cf. *Klass* §56; see also Loof 2006).

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

3.4.4 Whether an interference is necessary in a democratic society

The interference should be necessary in a democratic society. Again article 8-2 of the Convention provides the foundation[8]. For such interference the following applies (see *Silver*):

- a fair balance must be struck between the demands of the general interest of the community (a pressing social need) and the requirements of the protection of the individual's fundamental rights;
- the interference should be proportionate to the legitimate aim pursued.

On both issues member states do have a margin of appreciation.

The ECtHR may assess whether a fair balance was struck between the demands of the general interest of the community and the requirements of the protection of the individual's fundamental rights.

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

The interference is 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 realized with alternative less intrusive means, the ECtHR finds the intrusion disproportionate (*Olsson* §83, *Hatton* §97) [9]. This principle is also known as the subsidiary principle.

In *Erdem,* the ECtHR acknowledged that a precisely worded provision, specifying the category of persons whose correspondence must be monitored, in addition to restrictions on the

[8] "There can be no doubt as to the necessity, for the purpose of protecting national security, for the Contracting States to have laws granting the competent domestic authorities power" *(Leander* § 59)

[9] Loof (2005, 214) holds that the Court considers in the proportionality decision partly the way other countries are addressing similar issues.

use of the measure were such that interference in the communication between prisoner and layer were not disproportionate to the legitimate aims pursuit.
In *Weber*, the ECtHR ruled for the transmission of personal data obtained by general surveillance measures without any specific prior suspicion to allow the institution of criminal proceedings against those being monitored a fairly serious interference with the right of these persons to secrecy of telecommunications (*Webe*r § 125).
However, national security needs do not prevail automatically. In *Klass*, the ECtHR affirms that the danger of a law allowing secret surveillance poses a threat of undermining or even destroying democracy on the ground of defending it. Therefore, the European countries may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate (*Klass* § 49). The ECtHR has accepted that the existing legislation granting powers of secret surveillance is, under exceptional conditions, necessary in a democratic society in the interests of national security (*Klass* § 48).

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

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

3.4.5 Margin of appreciation

Provided the above, intelligence services can operate within certain boundaries provided by the European framework. According to the ECtHR's judgments, the requirements of morals varies from time to time and from place to place, especially in our era and national governments are in a better position to assess what circumstances should be considered a pressing social need which needs to be addressed with secret intelligence operations (*Handyside*; *Dudgeon* §52). Therefore, the ECtHR has accepted that national authorities make the initial assessment of the pressing social need in each case, and the means to apply; accordingly, a margin of appreciation is left to them. The scope of the margin of appreciation will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved (*Leander* § 59). 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 *Leande*r §59; *Weber* §106).
However, the decision of a national authority remains subject to review by the ECtHR (*Dudgeon* §49). In this respect, Arai-Takahashi (2002, p.83) argues that demonstrating good faith may be sufficient for national authorities to uphold their action. However, the ECtHR disagreed. It stresses that ECtHR' s oversight is not limited to ascertaining whether the respondent State exercised its discretion reasonably, carefully or in good faith. It also has to determine under Article 11 whether the interference is 'proportionate to the legitimate aim pursued' and whether the reasons adduced by the national authorities to justify it are 'relevant and sufficient' (*Refah Partisi* 2003).

3.4.6 Conclusions ECtHR

Measures interfering with the right to privacy as provided in article 8 of the ECHR and as interpreted by the rulings of the ECtHR must have some basis in law, accessible to the person concerned, foreseeable as to its effects, balanced against the interest of the individual, strictly proportionate to the intended purpose and should be subject to adequate safeguards.

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.

3.5 Privacy law in the European Union

The right to privacy in the EU Member States have their basis in the ECHR. Also many directives implement or specify the requirements for processing personal data of the ECHR such as the criteria of legality, legitimacy, subsidiary and proportionality (Koops and Leenes, 2005, p.127). These fair-processing standards are incorporated in the EU's governing directives on data protection, among others[10]:

- 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 (data protection Directive);
- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

Directive 95/46/EC is the general data protection directive. Directive 2002/58/EC particularises and complements Directive 95/46/EC. These directives provide the legal framework for private sector use of personal data, often including location data.
Member States may restrict the scope of Directive 95/46/EC and Directive 2002/58/EC for the processing of personal data concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law (see art. 3.2 and art. 13 Directive 95/46/EC and art. 1.3 and art. 15 Directive 2002/58/EC). For example, national government may decide that personal data processed for commercial purposes must be accessible to law enforcement and intelligence agencies to address severe criminal acts or to protect national security.

[10] Further, the Charter of fundamental rights of the European Union addresses the privacy issue (article 7 and 8). However, the Charter was part of the draft European Constitution, which has not been ratified.

Although the data protection directives may not apply to data collection to protect the national security, the data quality and security articles may be guidelines for managing personal data within intelligence services (see also IPTS 2003, 117).

3.5.1 Data quality measures

For data quality, the data protection directive rules that personal data should be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (art. 6.1.b Directive 95/46/EC). The processing should further be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (art. 6.1 c Directive 95/46/EC).
The controller must also ensure that the processing of personal data is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified (art. 6.1 d Directive 95/46/EC; see also Recital 26 Directive 2002/ 58/ EC).
Finally, the personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed (art. 6.1 e Directive 95/46/EC).

3.5.2 Security measures

Article 17 Directive 95/46/EC and article 4 of the Directive 2002/58/EC impose an obligation upon data controllers to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or unauthorised disclosure. The measures can be organisational or technical (see art. 17.1 Directive 95/46/EC; art. 4.1 Directive 2002/58/EC).
Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected (art. 17.1, see also art. 4.1 Directive 2002/58/EC).

3.5.3 Independent supervision

Directive 95/46/EC (art. 28) arranges for an independent supervisory authority with effective powers to intervene in the data processing.

3.5.4 Data processing principles extracted from Directives

Principles extracted from both Directives are (see also DPWP, 2007, p.7):

- specified purpose known before processing;
- use not incompatible with purpose;
- processing personal data should be fair: transparent what personal data is processed and by whom;
- personal data is no longer processed than necessary;
- data is accurate and up to date if this is relevant for the purpose of processing;
- data processing must be secure, and
- independent supervision with the power to intervene in the data processing

3.6 Conclusion

This chapter provides the findings of the study of relevant national and international legislation and case law. The United Nations, OECD and European privacy regimes clarify that privacy is a fundamental right, but may be invaded by other rights that serve other (more absolute) objectives of general interest recognized by a society. The right to privacy is in most international treaties recognized 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. An analysis of the European Convention of Human Rights, Convention 108, OECD principles, European Union Directives, judgments of the European Court of Human Rights results in six general principles that need to be satisfied to interfere with the right to privacy for purposes of national security (see also Westin 1967, p.370):

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.

Principle 5: Guaranteed accuracy of the data for the purposes of use.

Principle 6: Individual participation in the process whenever possible.

The first four principles stem directly from the ECtHR's interpretation of the ECHR. The principles 5 and 6 are addressed by Convention 108 requirements, OECD principles and European Union directives. These principles are the basis for the analysis of the case-studies.

4 Location privacy

Chapter 2 focused on general concepts of privacy. In this chapter we will further develop the concept with respect to location privacy. First, we provide background information on what may be considered location information. This is followed by a section that assesses the sensitivity of location data when they come to the scope of personal data. Then behaviour of users of location technology is addressed. Finally, a first attempt to categorize personal data and location data relative to their sensitiveness or level of revealing aspects of someone's private life is presented.

4.1 Location information

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, pp. 64-65). Location information may refer to the direction of travel, or to the identification of the network cell in which the terminal equipment is located at a certain point in time (Directive 2002/58/EC recital Number 14).
In the context of this research location information "means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service" (Article 2 (c) Directive 2002/58/EC). This includes the location area code, the cell-identity and the X/Y coordinates of the cell to which the device was connected (see also Explanatory Memorandum Decree ex article 28 WIV 2002).
Location privacy may be defined as: "the ability to prevent other parties from learning one's current or past location" (Beresford et al. 2003). It may also be defined as the ability to control the extent to which personal location information is being used by others.

The linkage of information to the earth gives information extra value. It 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. For many purposes, we need to know where what is. In the past a simple map was sufficient. With the increasing complexity of today's world the complexity of mapping also increases. Not only do we want to know more, we also want to know it more precise, more up-to-date and presented in a user-friendly way so that also laymen can understand it and use it. There is always a need to have access to answers to questions such as where am I, where are you, and what is where? These questions can be linked to property issues, situations of war, criminality, economic development, health, geographic planning, disaster management, and many more. Moreover, modern technology allows for information searches and analyses by geographic unit, making it extremely useful for geographic management and planning, for example disaster management purposes. In addition, both public (execution of policies) and private sector (profiling) linking a geographic element to the attribute may address the specific needs of the people in a geographic area more properly (see Rogers, 1993, p. 12). Longley (2001, p. 6) argues that almost all human activities and decisions involve a geographic component, and the geographic component is important.
An example shows what value geographic information adds to 'just' information. Imagine a situation of Mr X. His income is €100,000, end of the story: we cannot approach him physically and exploit the information. The linkage of an address to Mr. X allows the public tax office to send a tax form to his address, and the salesman of Mercedes-Benz a folder of its

latest models. He has now become more than his name; an asset that is easy to reach. When we include his attributes in a database with all inhabitants of area Y, we can map the income distribution, the distribution of sexes, or the distribution of people with a Mercedes-Benz. Another example is in health care: the knowledge that there is a relation between the characteristics of people and the likelihood for a disease is extremely valuable (see, for example, Snow, 1855). The location of the disease helps to find them and cure or prevent the distribution of a disease. These examples can be applied to many more human activities and decisions. Moreover, 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 et al. 2004, p.13).

Location information of mobile devices is also useful for law enforcement or security and intelligence services; who was at the time of the crime where, 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 network of the suspect. 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, 66). Examples of location information use of mobile devices, so-called Location based services, are

- Location services through Bluetooth (P.C. Hooftstraat scan) (see Tomesen 2007);
- To locate friends or stalk them (see Goldacre 2006) ;
- Find one when kidnapped (e.g., Bauer 2007);
- Keeping an eye on employees (Sciannamea 2004);
- Keeping an eye on your children;
- Locating people present near location of crime at time of crime committed;
- Mass message to all cell-phone in a certain area in instance of emergency, and
- Fleet management

4.2 How sensitive is location information?

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. Small-scale datasets are often of such limited detail that it does not provide the ability to link the geographic information to individuals: privacy issues are not likely to limit the use of small-scale information. The Dutch data protection authority considers data at the address level personal information (Registratiekamer 1996; Kamerstukken 25892 no. 3; CBP 2007). Therefore, this information is subject to privacy legislation. Initially, data at the zip-code level was not considered to include personal data (Kamerstukken 25892 no. 6). However, later it was argued that data at the zip-code level should be considered personal data if one is treated differently due to the linkage to these zip-code level data (see Kamerstukken 25892 no. 92c). Location information extracted from a cell-phone location may reveal at this zip code level where one has been at a certain point in time with whom, and for how long, directly touching upon one's privacy.

A name or an address alone may not impact on one's behaviour or private life. However, a combination of an address or 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 on 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 et al. 2004, p.13). This is especially annoying if the conclusions are inaccurate. The assumed visit to the coffee shop was in fact a visit to the supermarket just above the coffee shop. Or the visit to the tobacco shop was to buy a birthday card instead of Cuban cigars. This may have undesired consequences such as spam, or a unfavourable situation for one's health insurance.

4.2.1 Location information as special personal data

One may even argue that when the processing of location data refers to a location of a mental hospital or a church the location data should be categorised as the special, more sensitive, category of personal data. These data include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or concerning health or sex life. These are the 'special categories' of data, the processing of which requires special rules under Article 8 of the Directive 95/46/EC (see EU Directive 95/46/EC; see also EC Regulations No 45/2001; art. 6 Convention 108):

> "Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life." (art. 8.1 Directive 95/46/EC)

Although location information is not mentioned as a special category, in certain instances it may very well be considered to be in the special category of personal data. The Portuguese data protection authority, for example, has classified 'phone positioning data' as sensitive personal information (Korff 2002, p.85). But also in the other countries location data can be sensitive data since location data can reveal one's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. One may think of someone frequently visiting a mental hospital, a church, places where labour union boards or political parties meet, places known as frequently visited by gays, or a drug rehabilitation centre. In this respect, location data do reveal very sensitive data on individuals and as a consequence should be considered to be in the special category of personal data. One may argue that personal data are sensitive because of the circumstances in which they are processed not simply because of their content (Korff 2002, p.85 citing the UK Information Commissioner). Thus, the context to which location data are attached or used may be decisive for the privacy regime that applies to location data processing.

However, location data do not necessarily relate to the category of special personal data as specified by article 8 of the Directive 95/46/EC. Linking the location data to the membership of a student association or a sports club would not qualify as special personal data. Likewise, this would apply to most other data linked to a location. Location data without a context does not qualify as personal data. However, location data of a mobile phone can be relatively easily linked to an individual, which makes it personal data. Moreover, when the location data of a mobile device is linked to a specific sensitive context it may qualify as a special category of personal data.

But, Member States may restrict the scope of Directive 95/46/EC and Directive 2002/58/EC for the processing of personal data concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law. For these exceptional purposes, sensitive personal data may be processed.
In a comparative analysis of the implementation of Directive 95/46/EC in EU Member States, Korff (2002) found that privacy legislation in many European countries does not prohibit the processing of special personal data if the data subject has consented with it. For the processing of location data, this applies to even more countries. However, Korff (2002, p.88) found at least two countries that required additional formal requirements for all or certain sensitive data. In Greece, a permit from the data protection authority needs to be obtained for the processing of any sensitive data. In Portugal, such data may only be processed "when it relates to data which are manifestly made public by the data subject, provided his consent for their processing can be clearly inferred from his declarations" (art. 7.3.c Act on the Protection of Personal Data).

In the transposition of Directive 95/46/EC into national legislation several Member States added further categories of sensitive data, such as data on debts, financial standing and the payment of welfare benefits. Moreover, some Member States did not literally transpose the Directive, but broadened its scope by adding to 'revealing' the wording 'or refer to' (Spain; Korff 2002, p.84), or adding 'revealing directly or indirectly' (France; Korff 2002, p.84).
More specifically, the Netherlands has created different regimes for each type of special personal data. Churches and other associations based on religious or philosophical principles may process personal data revealing religious or philosophical beliefs unless the data subject has objected to such a processing (Art. 17.1 Wbp). The processing of personal data revealing racial or ethnic origin is allowed if this is to provide people belonging to a minority group a privileged position to ban or limit social imparity and the data subjects have not objected to such a processing (art. 18.b Wbp). Political parties and Labour Unions may process the personal data of their members (artt. 19.1 and 20.1 Wbp).

4.2.2 Location information as traffic data

Directive 2002/58/EC adds a special data category including location data: traffic data of communications. Traffic data are data that are required to enable the communications and those required for the billing process. It includes the phone numbers, duration of communication, time of communication and also information on the location of the cellphone at the time of calling.
Location data of a mobile device are traffic data because they are necessary to enable the transmission of communications (recital 35 Directive 2002/58/EC). In the context of the Directive 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. These traffic data reveal our 'habits and relations' (Penders 2004) to some extent at least.

4.2.3 Detailed location information in telecommunications

However, digital mobile networks may have the capacity to process location data, which are more precise than is necessary for the transmission of communications (Directive 2002/58/EC recital 35). For the processing of such more precise location data, the Directive applies a more strict regime. For, for example, value added services the processing of 'pre-

cise' location data is only allowed when subscribers have given their consent (see Directive 2002/58/EC art. 9).

Figure 4-1 shows the above in a graphical way. Location information at high levels of detail are indirectly identifying information. By itself or if linked to identifying information, general privacy law provisions apply to its' processing. If the information is further linked to a sensitive context the most restrictive privacy regulations may apply to the processing.

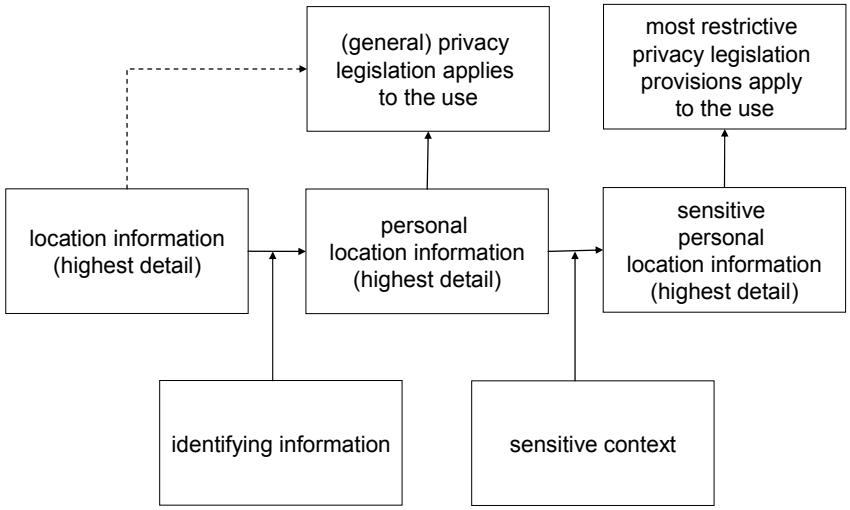


Figure 4-1 Categorization of location data

4.3 Location privacy and people's perception and behaviour

The use of location data of mobile devices is only one of the means that may interfere with the right to privacy. The intrusiveness of these means may vary. How intruding are such interferences with the privacy of individuals? Little research has addressed the sensitiveness of location information. In their review of several quantitative privacy researches, Raab and Bennett found that "concern about the keeping of information without their knowledge was particularly high, ranging from 94 to 59%, with respect to details about savings, earnings, court judgments, credit ratings, one's visitors, and medical history. The proportions were lower with regard to education and job history, what one buys, club membership, TV viewing, newspaper reading, and age, ranging from 38 to 13%. Doctors and the National Health Service [in the UK] were the organizations that respondents trusted most with their data (88%), and mail order companies the least (22%)" (Raab and Bennett 1998, p.267).
More recently, Koops et al. (2001) investigated in the Netherlands the 'criminal investigation v. privacy' perception of citizens. Two-hunderd-and-sixty-four citizens were asked in what situations what means may be used. The situations varied from small crimes to severe crimes, and from law enforcement (civil/public order) to national security. The means provided were linking data, camera surveillance, house searches and wiretapping.

Citizens consider acquiring and merging data as well as camera surveillance permissible in 60 and 65% of the cases. House searches and wiretapping appear to be accepted in 48 and 39% of the cases. Although the sample was non-representative for the Netherlands, it suggests an order of diminishing sensitiveness of data:

- wiretapping;
- house searches;
- merging data sources, and
- camera surveillance.

However, in the above mentioned researches, location information was not considered. Verhue (2007) performed the Dutch National Freedom Investigation 2007, commenced by the 4 and 5 May committee. He analysed the results of 1009 questionnaires asking about the extent to which citizens would accept government interference with their privacy. One of the questions included a list of a variety of privacy-intruding means for which their intrusiveness needed to be assessed by the respondents. The researcher found 'a striking common sense' in the respondents' answers for the extent of privacy infringement of each means (Verhue 2007, p.24).
The group of most infringing means, scoring between 2.5 and 2.75 on a 1-3 privacy-infringement scale, was: wiretapping; content of email and internet traffic; house search of suspects; and taking a suspect in detention. The following group, scoring between 2.25 and 2.5 on a 1-3 privacy-infringement scale, was: location determination through cell-phone; precautionary body search; acquiring and storing dna-profile of everyone. The third group, scoring between 2 and 2.25 on a 1-3 privacy-infringement scale, was: location determination through license plates of cars; and exchanging data from airlines. The final group, scoring between 1 and 2 on a 1-3 privacy-infringement scale, was: camera surveillance in public space; and the requirement to carry identification papers from age of 12.
Further, Verhue (2007, p.25) found that the acceptance of using these means to address terrorism was relatively low for cell-phone tracking (63%), checking all email/internet traffic (55%), and eavesdropping (cell) phone traffic (50%).

	2005	2007
Camera surveillance	88%	94%
Internet & email surveillance	55%	55%
House searches	49%	87%
Ubiquitous phone tapping & eavesdropping	45%	50%
Locating cell-phone	-	63%

Table 4-1 Acceptance of means to increase security in exchange of liberty (source Veldkamp 2005; Verhue et al. 2007)

From Verhue we learn that citizens in the Netherlands consider locating cellphones as a significant privacy infringing activity. One might suspect that citizens will behave accordingly and prevent using a cellphone as much as possible. In the next section, we will see that this hypothesis is not supported by location privacy behaviour research.

4.4 Location privacy behaviour research

Several researches have addressed the behaviour of people when using location based services. One of the issues involved in these researchers is the extent to which, from a theoretical perspective, the processing of location information may interfere with an individual's privacy. However, how private do individuals consider 'their' location information as private information?

Danezis et al. (2005) assessed the value of location information in an experiment context. They found that most participating students would allow their mobile phone to be queried for its location every few minutes, 24/7, for 28 days for at most (the highest bid) 30 pounds with most bids below 10 pounds (€15). This was for scientific use. When participants were asked to 'sell' their location data for commercial use, the bids were raised to an average of 20 pounds (€30). Similar research across Europe by Cvrcek et al. (2006) arrived at comparable results. In addition, Cvrcek et al. (2006) found that when extending the tracking from one month to a year the average bid for commercial use went up to several hundreds of euro. Although the researchers acknowledge that students may have a lower privacy expectation than ordinary citizens, the researches suggest that location information can be acquired from 'innocent' citizens against a small monetary return.

Krumm (2007) found that over 200 people in his company were easily convinced to allow the gathering of GPS data recorded in their car for two weeks in return for a 1 in 100 chance of winning a MP3 player. Moreover, Barkhuus et al. (2003a) found through experimental case study with 16 participants that people are positive towards location-based services as long as they perceive them to be useful (see also Chang et al. 2006, Kaasinen 2005, Barkhuus et al. 2003b). Especially 'user controlled' services like find-a-friend are positively assessed by the user (see Colbert 2001; Barkhuus 2004).

Other research confirms that users of a cell-phone equipped with GPS find a reminder service given at the right place useful (see Ludford et al. 2006, pp. 895-896). For example, when one is close to a store a text message may remind the user to buy a wanted item. Barkhuus et al. (2003; see also Barkhuus 2004) further found that in their experimental case study location-based services focusing on closed or group environments were considered to be less intrusive than others such as commercial adds 'discount message at the nearest restaurant', or 'AT&T wishes you a happy birthday' message.

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. On the contrary, Danezis et al. (2005) did not find any commercial successful location service.

These researchers suggest that the privacy expectations of user 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 what is being done to their personal data (see Barkhuus 2004). Consequently location privacy may not be as highly valued as many suggest, and continuous surveillance of terminal devices not as intruding.

The extent to which currently people behave does not suggest that something like privacy-awareness of individuals exist, let alone is increasing. Research suggests that quite the opposite is true, especially when those value adding location based services are offered that are desired by the user.

4.5 Location information compared to personal data

Based on the researches on the value of location data, the categorisation of personal data in legislation, and on other studies aiming at categorising different types of personal data, one may come to an initial order of sensitivity for data:

1. sensitive data; data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or concerning health or sex life and data in the category of the content of communications (letter, email, voice-mail, phone conversations);
2. real-time data (location, financial transfers);
3. historical location data of cell-phone; traffic data of cell-phone; details about savings, earnings, court judgments, credit ratings, one's visitors, and medical history;
4. education and job history, what one buys, club membership, TV viewing, newspaper reading, and age;
5. identifying data; data that determine the identity of individuals and that connect people and situations: name, address, sex, birth date, administrative characteristics such as phone number, bank account number, client number, license plate number.

These categories can be further specified with respect to the components Type of data, Time information, and Context information.

Type of data

Type of data comes directly from legislation. Three categories are distinguished: (1) sensitive personal information, (2) personal information, and (3) non personal information.
The first category includes data that is in itself considered to be sensitive such as health information. 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. Location information may indirectly identify someone, especially if the location information is at a high level of detail. An address may be an example, but it also applies to detailed location information showing one's home. It depends on the level of detail of the location data (i.e. large scale v. small scale data). Generally, data at the zip-code level is not considered personal information. This implies that the current levels of detail for mobile devices, at best 50-100 meter, would qualify as non-personal data. Finally, non-personal data does not interfere with privacy. For example, location information at a 1:1,000,000 scale will generally be considered non-personal information.

Timeliness

Time may have similar characteristics as location. The knowledge of what one is doing now may be considered private today. But 20 years from now, this information may 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 until the observed individual shows unusual behavioural patterns. For example, if he is more than frequently visiting a nuclear power plant, or increasing the number of phone calls to certain people. These may indicate the preparations of an attack.
Barkhuus et al. (2003) consider information referring to a person's position a specific attribute of identity, similar to name and social security number. Generally, real-time location in-

formation 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 this 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 the former colleague accidently revealed this information, Rasmussen was fired and had to give up his number one position in the Tour de France. Thus, also linking rough location information to other information may result together in a set of information that can be considered personal information.

Context

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. Context has been addressed in section 4.2. If personal location information can be linked to a certain context (e.g., a church), this may impact the applicable privacy regime of the information. 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 the 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 Tanja Nijmeijer (a supposed member FARC). 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. Probably a different standard is applied to family and friends then to direct marketing companies.

Another component not specifically being addressed in research or legislation is information on what one is doing somewhere. Westin (2003, 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, 445).

The context or circumstances determine whether location data may categorise as non-personal data, personal data, or sensitive personal data. The processing of location information may be among the most sensitive categories of personal information, e.g., 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. Figure 4-3 provides guidance at the conceptual level. However, in specific instances a different categorisation may apply.

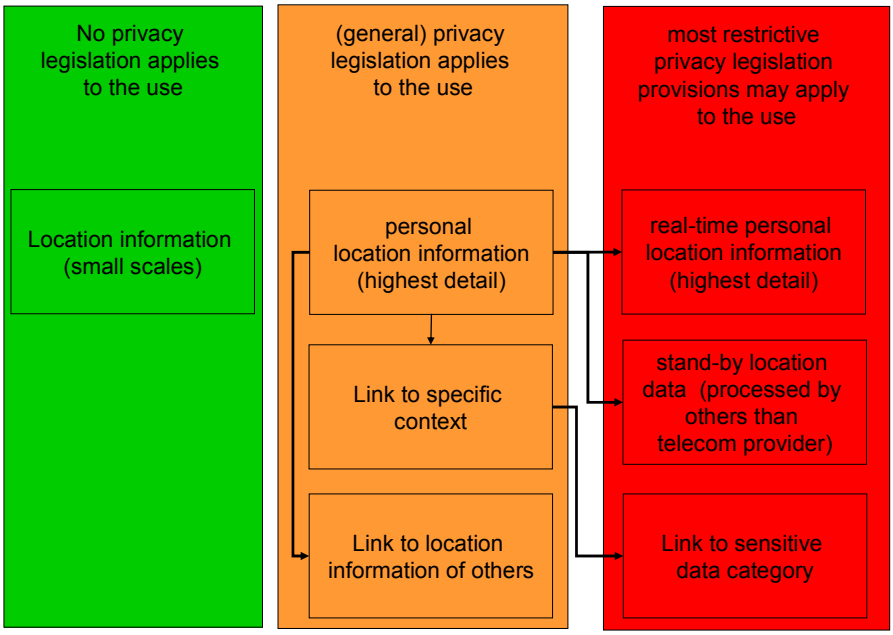


Figure 4-2 General categorisation of location information and applicable legal regime

4.6 Location privacy & theory

Location privacy involves both informational privacy and the physical privacy at a location (right of autonomy and/ or seclusion). For the privacy of users of mobile devices both aspects are relevant, but relates to the timeliness and goal of processing the location information. If the knowledge of where you were, when, with whom, and for how long is only ex-post included in a database, which is used to update one's profile, the individual will still be at all times in control of his movements, and no one is to interfere with his behaviour. However, his informational privacy may be intruded. Further, based on the profile created by infringement of his informational privacy it may be decided to track and trace a certain person. With real-time tracking, the current position of the mobile device is revealed and the direction it is heading to. In these instances the tracker has the ability to interfere directly in someone's behaviour. This may then result in an infringement of his physical privacy. The informational privacy is likely to be less relevant in this context.

Infringement of / Interference of	Physical privacy	Informational privacy	Relational privacy
(cell)phone conversation		(X)	X
(cell)phone location ex-post		X	
(cell)phone location real-time	X	X	
(cell)phone traffic information		X	

Table 4-2 Linking data category to privacy concept (1)

Depending on the characteristics of location data it can be just data, personal or sensitive personal data. Consequently, control over location data can be considered to contribute to

one's physical privacy, or informational privacy, each with different data processing regimes (see Table 4-3).

Type of data	Privacy category
sensitive data content of communications	Informational privacy Relational privacy
real-time data (location, financial transfers)	Physical privacy
historical location data of cell-phone in stand-by mode	Informational privacy
historical location data of cell-phone (actively used) traffic data of cell-phone details about savings, earnings, court judgments, credit ratings, one's visitors, and medical history	Informational privacy Relational privacy Informational privacy
education and job history, what one buys, club membership, TV viewing, newspaper reading, and age	Informational privacy
identifying data	Informational privacy

Table 4-3 Linking data category to privacy concept (2)

4.7 Summary

Location information comes in many shapes and sizes. The extent to which the use of location information interferes with the right to privacy depends on the type of information, the level of detail of the location information, the timeliness of the information, and the context to which it is linked. As a consequence, the extent to which location information can be considered personal data or sensitive personal data varies from situation to situation. For example, concerning telecommunication data, Directive 2002/58/EC distinguishes two types of location data: traffic data and location data. Traffic location data is necessary to enable the communication. 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. However, linking traffic data to a specific context and time (who did you call yesterday at 8pm) may change the non-personal traffic data into personal information to which privacy restrictions applies. In a general sense, the use of highly detailed (e.g., scale 1:500), real-time location data linked to a sensitive context, such as a church, can generally be expected to be at a higher 'privacy level' than less detailed data (e.g., scale 1:25,000) of a decade ago without a link to a specific sensitive context.

In addition, different people may have different privacy perspectives. Research on telecommunication use and location based services suggest that people generally do not value location privacy as high as one may expect. Walters observation may also apply to location privacy: Generally privacy's importance is not recognized by individuals "until it is taken away… [..]" (Walters 2001, p.8).

5 National security

This chapter addresses the concepts of national security. Concepts since the definitions of national security in general and terrorism more specific, are not uniform with each other. European Union, United Nations, as well as the views of academics are provided. Focus in this chapter is on national security in the sense of combating serious crime and terrorism. Disaster management in another sense is not the primary objective of this chapter.
One of the core means to satisfy national security needs is surveillance. This chapter identifies possible ways of surveillance and provides positive and negative aspects of these specific forms of surveillance.

5.1 Security

The term security includes a broad spectrum. It can be regarded as a state of being secure, free from threats as fear, damage, intimidation, among others (Venice Commission 20007). Charter 5 of the ECHR addresses the right for security ("Everyone has the right to liberty and security of person") (see Frattini 2007). One may think of international security, home security, information security, network security, financial security, human security, food security (wikipedia). One may also think of security with respect to natural disasters such as floods, traffic security, security of access to public services, but also of communication security for example in order to have guarantees that one's bank account is only accessible to himself. Also security with respect to protection against crime and even social security are among the general concept of security. In the context of national security, internal and external security can be distinguished. Internal security threats are typically domestic threats, while external security relates to threats originating from abroad. However, current globalisation has blurred the clear distinction between the two (see also Venice Commission 2007).
Further, there is a difference between perceived security and real security (see Boutellier et al. 2005, p.8-9). Perceived security relates to the security perception of individuals or groups. Visible enforcement officers, security agents, detection booths, nicely mowed gardens, and name tags attached to one's front door may attribute to a secure perception. Poorly maintained buildings, and groups of people with 'intimidating' looks (piercing, tattoos, scooters etc) may influence the perception negatively. Real security comes down to the facts: number of registered crimes, harassments, and other nuisances.

5.2 What is national security?

National security is an extremely flexible notion. In order to assess national security in relation to privacy, its definition is important (see also ROB 2005, p.39). However, 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. 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. He states that these issues are regarded by most if not all governments as legitimate national security concerns. 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.

The continuance of the state and its values is of great value. 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[11]). Therefore, 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 and Kamerstukken 25877, nr. 58; UN Economic and Social Council *Siracusa Principles* (article 29)).

The ECtHR has accepted that the following activities may justify measures to protect the national security (Kamerstukken 25877 nr. 58, p.31; see also Loof 2005, p.256):

- violation of state and military secrets;
- distributing inflammatory writings under military;
- maintaining the discipline within the military and the administration;
- inciting and approving violence;
- performing neo-Nazi activities;
- performing terrorist activities;
- publishing secret information and writings that may harm the functioning of a state's intelligence;
- prohibiting and punishing expressions that provide a voice to separatism or terrorism, among others, that harm the national unity, and
- secretly peering around and surveil telecommunication by security services

In *Klass* and *Leander* the ECtHR has accepted that even though national security was at the moment of the intrusion of the human right not at stake, still measures protecting the national security could be taken to prevent a situation that would threaten the national security.

5.3 Aspects of national security

5.3.1 Timeliness of society's norms

The elements supposedly threatening national security change throughout time. 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. Anyone supporting activities that are assessed to be in 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 norms change overtime and accordingly the subject of surveillance by intelligence agencies change. 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

[11] The ECHR nor the European Court of Human Rights gives a definition of national security.

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 arms into Iraq increased war concerns and in 2005 the assassination of Theo van Gogh had a similar impact on terrorism concerns (see Table 5.1).

Year Concern	2002	2003	2004	2005	2006	2007
War	43	67	45	36	35	37
Terrorism	42	49	49	61	57	47
Crime	40	35	35	36	25	31
....						
Violation of fundamental human rights	15	13	13	15	14	15
Influential event	9/11	Iraq		Van Gogh		

Table 5-1 Concerns of Dutch citizens (in %) about issues in the world (source Veldkamp 2002, Veldkamp 2003, Veldkamp 2004, Veldkamp 2005, Verhue et al. 2006, Verhue et al. 2007)

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. Once the law is in place it will be difficult to change or replace it even when the threat has disappeared (see IPTS 2003; Koops 2006, p.36).

5.3.2 National security and culture

The attitude towards national security (or specifically surveillance) differs between individuals and societies. "Many cultural beliefs support the legitimacy of surveillance. Consider statements as "I have nothing to hide," " It's for my own good," "I support the goals", "It's just the way they do things here", they have to do it…", "they promise to protect confidentiality" (Marx 2003, 370-371). "Public acceptance of such [national security] measures will depend on the level of terrorist threat and on the nature and extent of actual abuse of civil liberties" (Margulis 2003, 251).

5.3.3 Changing national security threats

Before 9/11 national security issues were often related to organisations that operated within particular geographical boundaries. The ETA, IRA, Hamas, Hizbollah are examples of such organisations. However, at present day (after 9/11/01 (US), 10/12/02 (Bali, Indonesia), 3/11/03 (Madrid, Spain), 7/7/05 (London), 7/23/05 (Sharm el-Sheik, Egypt)) terrorism as a threat to national security has lost its relation with a certain geographic area: terrorists today 'know no bounds' (see also Loof 2005, p.247, cf. Dempsey et al. 1999). These terrorists aim through mass destruction to destabilize democratic states. In order to arrive at these goals, the current terrorist is willing to sacrifice his or her life to die as a martyr. The protection of

the national security cannot suffice to punish ex-post, but require preventive means to combat this 'catastrophic terrorism' effectively (Loof 2005, p.248).

However, although not defining terrorism, Coolsaet et al. (2006)'s assessment suggests that the number of international terrorist attacks and victims, excluding Iraq, is declining (with 33% resp 40%), supporting the feeling that there is a gap between the suggested increasing threat and reality. More specifically, it is domestic terrorism that appears to be the real threat, and this is not a threat of global nature but largely concentrated in the Middle East (Coolsaet et al., 2006, p.4).

5.4 When is it necessary within a democratic society?

The Universal Declaration of Human Rights (art. 12), and the ICCPR (art. 17) are the basis for allowing national security interferences with the right to privacy. The UN Economic and Social Council developed these further in the Siracusa principles. Also the Johannesburg principles can be mentioned in this respect. Both principles are discussed here.

5.4.1 Siracusa principles[12]

The UN Economic and Social Council addresses national security in its' *Siracusa Principles*[13],[14]. In article 30, it stresses that "National security cannot be invoked as a reason for imposing limitations to prevent merely local or relatively isolated threats to law and order." National security can also not be used as a pretext for imposing vague or arbitrary limitations and may only be invoked when there exists adequate safeguards and effective remedies against abuse (article 31).
Finally, the Siracusa Principles (art. 32) emphasize that "The systematic violation of human rights undermines true national security and may jeopardize international peace and security. A state responsible for such violation shall not invoke national security as a justification for measures aimed at suppressing opposition to such violation or at perpetrating repressive practices against its population."

5.4.2 Johannesburg principles

In 1995, a group of experts in international law, national security and human rights developed principles based on international and regional law and standards relating to the protection of human rights, evolving state practice (as reflected, inter alia, in judgments of national courts), and the general principles of law recognized by the community of nations (Johannesburg principles). Although the principles do not address privacy (focus is on national security, freedom of expression and access to information) they may provide some guidelines how national security relates to other human rights. These principles have been endorsed by the UN Special Reporter on Freedom of Opinion and Expression, in his reports to the 1996, 1998, 1999 and 2001 sessions of the United Nations Commission on Human Rights, and referred to by the Commission in their annual resolutions on freedom of expression every year since 1996 (Article 19 1995, p.1).

[12] A group of 31 experts in international law, convened by the International Commission of Jurists, the International Association of Penal law, the American Association for the International Commission of Jurists, the Urban Morgan Institute for Human Rights and the International Institute of Higher Studies in Criminal Sciences, met in Siracusa, Sicily, in 1984 to consider the limitation and derogation provisions of the International Covenant on Civil and Political Rights (website SIM)
[13] United Nations, Economic and Social Council, U.N. Sub-Commission on Prevention of Discrimination and Protection of Minorities
[14] Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights in chapter I. Limitation Clauses, section B. Interpretative Principles Relating to Specific Limitation Clauses, under vi. "national security"

The preamble of the principles recognizes that the most serious violations of human rights and fundamental freedoms are justified by governments as necessary to protect national security.

Principle 1.3 reads:
To establish that a restriction on freedom of expression or information is necessary to protect a legitimate national security interest, a government must demonstrate that:

(a) the expression or information at issue poses a serious threat to a legitimate national security interest;
(b) the restriction imposed is the least restrictive means possible for protecting that interest; and
(c) the restriction is compatible with democratic principles.

Thus, it recognizes the principle of subsidiary.

The Johannesburg principles also address legitimate national security interests (Article 19 1995, principle 2):

> (a) A restriction sought to be justified on the ground of national security is not legitimate unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government.
>
> (b) In particular, a restriction sought to be justified on the ground of national security is not legitimate if its genuine purpose or demonstrable effect is to protect interests unrelated to national security, including, for example, to protect a government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest.

5.4.3 The European Court of Human Rights

The ECtHR has ruled that "the mere fact that 'information' or 'ideas' offend, shock or disturb does not suffice to justify that interference [..]" with the right to privacy for national security purposes. However, actions that offend the values of a society and incite to violence to change these values justify measures to protect national security (Loof 2005, p. 338; see also *Sürek* § 40).
Under exceptional conditions surveillance of communications is necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime (*Klass*). Questiaux has argued that "Exceptional circumstances will mean (…) circumstances resulting from temporary factors of a generally political character which in varying degrees involve extreme and imminent danger, threatening the organized existence of a nation, that is to say, the political and social system that comprises as a state" (Questiaux 1982, p.8 cited in Loof 2005, p.32).

5.5 Means to satisfy national security needs

National security can be protected through varied means. Wikipedia mentions:

- using diplomacy to rally allies and isolate threats;
- maintaining effective armed forces;
- implementing civil defence and emergency preparedness measures (including anti-terrorism legislation);
- ensuring the resilience and redundancy of critical infrastructure;
- using intelligence services to detect and defeat or avoid threats and espionage, and to protect classified information;
- using counterintelligence services or secret police to protect the nation from internal threats.

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). Anyone supporting activities that are assessed to be in 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.

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. "By gathering data about people and their movements they strengthen 'the surveillant assemblage' - a term describing the relationship between heterogeneous surveillance technologies that "'work' together as a functional entity", but do not have any other unity" (IPTS 2003 referring to Haggerty and Ericson 2000, p.605).

Some examples of potential sources for the surveillant assemblage, to be scrutinized around the clock are (see also O'Harrow Jr. 2005, p.29, 166, 222, 248, 281-285, 293; EU 2005, p.4):

- surveillance cameras everywhere (highway, coffee shop, public areas, gas stations, supermarkets, shopping malls, and so forth: travel activity, personal network (who were you with) & physical characteristics (clothing, car, etc)
- Closed Circuit TV (CCTV) and face recognition
- WiFi and computers: travel activity
- Mobile phones: travel activity, personal network and rating
- Magnetic strips (public transportation: travel activity, office entrance: effective work activity (lunch time etc))
- Credit cards: spending pattern
- Tollbooths: travel activity
- Internet: internet activity (sites visited, frequency, time spent, newspaper site: everything your read, everything about you (memberships, articles on or by you)
- TiVo machine: everything you watch on TV
- ATM: amount, time, frequency and where
- Frequent flyer passes
- Discount or loyalty cards
- Bank deposits

- Parking meter: electronic tickets
- Books borrowed from the library (Mein Kampf, Das Kapital, Koran, Theo van Gogh, Autobiography Bin Laden)
- Email: recorded and monitored by e-mail provider, or employer
- Phone (conventional): personal network, your name, voice and key words that you use
- Electronic car keys: antitheft system, but potentially the tags in the key can be scanned and become multipurpose.
- RFID tags in everything (e.g., medicine, car keys, cloths, electronic devices, e-tickets, etcetera).
- Personal security systems in cars allowing two-way communication, which can be used to eavesdrop the car.

Similar to the privacy categorisation in this research, 'soft' surveillance may be categorized as physical surveillance, dataveillance and psychological surveillance.

5.5.1 Physical surveillance

Physical surveillance is surveillance by observation: close observation, especially of a suspected person (Marx 2002, p.10). Westin defined it as: "the observation through optical or acoustical devices of a person's location, acts, speech, or private writing without his knowledge or against his will" (Westin 1967, p.68). This includes tapping the computer (Westin 1967, p.79). It is an active way to track individuals. Physical surveillance implies knowing where the 'subject' is at all times, and especially where he goes when he wants to be alone (e.g., physical shadowing). In the past this was realized with a special agent dedicated to follow a suspect of suspicious subject. Already in the 1960s, it was possible to "tag" persons so that they can be followed more efficiently and with less risk of discovery through fluorescent powders, or a miniature radio-signal transmitter) (Westin 1967, p. 69). Today, communication technology networks like WiFi networks, RFID networks, cell-phone networks, together with active GPS in mobile devices allow for an even more efficient and secure way of tracking and tracing someone. It is no longer necessary to place the tag at a person; the person carries the tag with him without knowing that his PDA, laptop, or cell-phone functions like that.
The physical surveillance can also be accomplished passively through the use of a CCTV network or the monitoring in a factory, where on a incidental basis people's whereabouts may be followed.

5.5.2 Dataveillance

Another aspect of surveillance is the dataveillance. Dataveillance may be defined as the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons (see Clarke 1994; Levi and Wall 2004, p.200; Marx 2002, p.12). It can be used to make an initial assessment of potentially dangerous individuals or groups, or to obtain a more detailed or complete picture of a person selected for physical surveillance.
Closely related to dataveillance is profiling. Profiling is attributing certain characteristics to a person based on facts, and his behaviour. The profile enables authorities and others to target the individual accurately and may predict to some extent the likelihood of future actions. O'Harrow Jr. has described nicely the impact of profiling and dataveillance:

> "When the artificial intelligence comes to understand a customer, that insight doesn't only have to be applied to criminal activity. It can also be programmed to anticipate when a pay check is coming in, and whether someone is getting a pay raise. Over time it will learn when an individual's family tends to go on vacation. It can calibrate how much a bachelor typically spends on Friday nights and where. By analyzing changes in his behavior, it could also say when he has tied the knot. That of course could give the marketers a chance to look for signs the honeymooners intend to have a baby." (O'Harrow Jr., 2005, p.265)

O'Harrow Jr. (2005, p.208) also suggests that such potential interferences are not utopian since the FBI has in addition to the public databases access to a wide variety of private databases (from Choice Point, Seisint, LexisNexis, Acxiom, airlines, Internet service providers, credit reporting agencies, libraries, banks, apartment complexes and grocery stores).
An increasing number of databases are interoperable. European Security Research has assessed that more than 80% of the world's database content is in unstructured largely textual format (ESRAB 2006, p.46). That is 20% is in a structured format which is potentially interoperable.
Location information is an important aspect in the dataveillance. Who was where when was already mentioned before. But also how can we find the individual, where does he live or where is he now is valuable information for both the public and private sector. For example, location dataveillance may reveal a personal network, or one's behaviour. However, although data mining may reveal an unknown pattern or relationships between data elements, it cannot reveal the value or significance of the data to the user (White 2003). The computer is unable to reveal the reason behind the found relationship (White 2003).

5.5.3 Psychological surveillance

Psychological surveillance is "those scientific and technological methods that seek to extract information from an individual which he does not want to reveal or does not know he is revealing or is led to reveal without a mature awareness of its significance for his privacy" (Westin 1967, p.133). Examples are polygraph tests (lie detectors), LSD and other drugs. Psychological surveillance may also be known as extraction. Extraction is to enter into a person's psychological privacy by requiring him to reveal by speech or act those parts of his memory and personality that he regards as private (Westin 1967).
This research does not address psychological surveillance.

5.5.4 Issues questioning intelligence operations

Operations addressing national security threats may compare with operations addressing emergencies under emergency law (*noodwetgeving*) as identified by the ROB (2005, p.44). It is very difficult to make an objective threat assessment, the need and effectiveness of the measures are difficult to measure, a temporary stop of the activities will therefore be problematic, and political responsibility may not adequately be fulfilled.
Due to the nature of a security and intelligence agency, successful secret operations ought to remain secret. Assessing the need for intelligence operations is subject to a large degree of subjectivity. For a risk assessment not only factual information is necessary, also 'speculative' or 'soft intelligence' is required. Such soft intelligence may come from informants, infiltrants or even unidentified individuals. Security officials need to assess the reliability of the information provided and arrive at a reliable risk assessment for a possible security risk (Venice Commission 2007 §86-87).

In addition, useful statutory definitions of what exactly national security is, are scant. This makes it difficult to demarcate the boundaries of the activities of the security and intelligence services. Provided the assumed natural tendency of security and intelligence agencies to over-collect information this potentially stimulates abuse of power (Venice Commission 2007 §4, 5 & 85).

5.6 Surveillance benefiting national security

Surveillance has both positive and negatives impacts for society. Physical surveillance enables one to know where the potential risk is, what he does with whom and provides the possibility to intervene if this appears to be necessary. Location surveillance further helps to execute personal network analyses and travel behaviour of suspects in combination with context information (Akerboom 2003).

The highly detailed personal records and profiles may provide "instant credit, cheaper mortgages, a panoply of shopping options, and even detailed and accurate phone books" (O'Harrow Jr. 2005, p.41). These profiles may also result in preventing actions with a negative impact on society. For example, [Seisint] created a "terrorism quotient" that tagged certain individuals as having a "High Terrorist Factor" score. [Seisint] gave federal and state authorities 120,000 names of people with the highest scores, along with a "1 percent list" containing the names of the 1,200 people deemed the biggest threats. That refined list provided leads in scores of investigations and led to some arrests. [..] five of the names [..] generated were hijackers on the planes crashed on September 11" (O'Harrow Jr. 2005, p.102).
Also other criminal activity may be resolved with the help of dataveillance. For example, the Beltway Sniper, who was active in Washington DC area in 2004, was eventually caught with the help of facts from the crime scenes, expected profiles of the suspect and a database. Based on a combination of information such as rifle .223 caliber, 'You don't go where you don't know' (expert knowledge), an army postal address, assumed ties of the suspect to the Northwest, a first name came out of the system but this person was assessed by experts to have the wrong profile. A further analysis on same or similar names with the expected profile resulted in the name and location of the murderer found (including dirty former police car, and .223 calibre slugs from the killing rifle (O'Harrow Jr. 2005)).
Similarly, LexisNexis found a house in Florida that several of the 9/11 hijackers had shared (O'Harrow Jr. 2005, p.225). This information may have prevented 9/11 when the links between these people and '9/11' would have been clear.

The European Security Research Advisory Board has identified positioning and localisation of individuals and goods as one of the eleven key technologies required to be integrated into various systems in order to deliver security mission requirements (ESRAB 2006, p.48). The technology domain of navigation, guidance, control and tracking is one of the 23 priority technology areas they identified (ESRAB 2006, p.50).
Many cases show the value of location data in solving crimes because a certain mobile device belonging to someone was at the moment of the crime at a certain place close to the crime scene. The value may show ex post (where were you when a certain activity took place) or real-time (where are you now?).

5.7 Potential impact of surveillance on society

It is commonly accepted that for purposes of national security, privacy may be invaded (see Loof 2005, p.1; IPTS 2003, p.141; Blok 2002, p.278; Walters 2001, p.19; Raab and Bennett 1998, p.265-266; Westin 1967, p. 26). In order to be effective, not only criminal but also innocent citizens will be subject to surveillance. If an appropriate *profile* of a terrorist in the making has been found, how many of these need to be tracked? Imagine the profile of a terrorist, living in the Netherlands (16 million people), of non-western origin (1.7 million people), Islamic religion (850,000 people), and second generation immigrants (147,000 people). One percent of the people with this profile may be a potential supporter of extremist standpoints. If out of this group, another 10% may consider committing an activity that has a major impact on Dutch society, then, based on this profile alone, at least 147 people need to be tracked. Only a few of the 147 may be a real danger to society, but also the innocent are going to sacrifice (some of) their privacy (O'Harrow 2005, p.139). Further, 'Credit scores' exist to assess the risk that a borrower might default (O'Harrow Jr. 2005, p.224). Another example concerns a US State Senator, a professor, and graduate student all with the same name who keep getting stopped, detained, missing flights and having trouble booking flights because they have a name similar to someone on the No Fly list. Even if you are a woman (Johnnie Thomas) and there is a man on the list (John Thomas), you will be stopped (O'Harrow Jr. 2005, p.228/31). "Even a document from the FBI attesting to the authenticity of her identity was ignored by airport security officials" (O'Harrow Jr. 2005, p.231). Thus, security officials may trust the outcome of the computer more than official documents.

From one privacy scholar we learn that in the short term surveillance may lead to adapted behaviour of human beings resulting in *a loss of autonomy*. The more surveillance (governmental and private) we tolerate, the more we are heading towards a so-called 'panoptic-society'; the permanent awareness of being observed that ensures power to take effect automatically: mainstreaming of citizens behaviour (Peissl, 2002). "As soon as technical means like video systems in public places or wire-tapping of telecommunications systems will be perceived by ordinary people in their everyday lives, they will try to circumvent those surveillance systems" (Peissl, 2002). In the long run surveillance may prevent any 'driving momentum' in society in societal, cultural and economic terms: non-conformist behaviour is a necessary driving force for societal development. If our societies stop to develop they will perish (Peissl, 2002).

However, in Chatham in Kent (UK), and also in Cork city and many other places in the UK there is a widespread use of CCTV cameras in town centres, public places, and private housing estates. But, citizens seemed to be very positively disposed towards having this surveillance. It seemed that most people spoken to felt happier and more secure knowing that "someone" is keeping an eye on things (Contribution of Darius Bartlett to the EGIP discussion list, 26 April, 2006). This is despite that the use of the CCTV seem not be as effective as expected (McSmith 2008).

5.8 Effectiveness of surveillance in protecting national security

Successful surveillance implies that the terrorist can be found, tracked and stopped. Terrorist, however, may use (a) strategies of avoidance or (b) use preventive technologies. They may prefer personal meetings and communication rather than chat rooms, use cash instead of ATM machines and credit cards (see O'Harrow 2005, p.265). They may further use privacy enhancing technologies or ancient ways of communication (mouth to mouth), which cannot be tracked down to a location. "From the attacks of September 11, 2001 (and Madrid March 11, 2003, and London July 7, 2005) we had to learn that the involved persons lived 'normal' lives for years. Hence they could not be detected" (Peissl 2002; see also Akerboom

2003 'couleur locale'). Further, before the attacks in the London Underground in 2005, the terrorist threat to the national security was at its lowest point since 9/11 (ROB 2005, p.45). This raises the question of the effectiveness of the surveillance measures of intelligence services.

5.8.1 Secondary use of information.

Especially in the context of national intelligence, accurate information is of evidential importance. National security and intelligence services would need to find potential terrorists, or assess the risk that one may be one. This assessment relies on the available data on suspects to the agency. They may rely on massive (private and public) databases including personal data, but not collected for national security purposes; a so-called secondary use. Private sector may have collected the data for marketing purposes, which allowed the collection of less accurate data (but sufficient for marketing purposes). One of the key questions is: Is this collected information sufficient for national security purposes? In many instances the answer would be no.

One example of secondary use is found in the US, where names of registered voters were compared against lists of known felons, deceased people, and duplicate registrations. "8,000 of the 66,000 people identified as felons were in fact Texans convicted only of misdemeanors and therefore entitled to vote" (O'Harrow 2005, p.127). It was concluded that "the cleansing effort had a disproportionate impact on African-American voters" (O'Harrow 2005, p.128). The impact may remain unknown, but it has been suggested that Bush Jr. would not have defeated Al Gore by 537 votes in Florida if the exclusion list had not existed or would have contained correct information.

Other causes of wrongly interfering with someone's life may be the query that is addressed by the data in the database. When is the threat to national security expected and from whom or what? What should be the focus of intelligence? How reliable are the answers to these questions, and how reliable are the sources used? Again O'Harrow (2005, p.242) shows that the current focus on a certain profile may allow the axe murderer with a clean record to get on the airplane and commit his crime, because "that is not the person we are trying to keep off that airplane at the moment".

Also secondary use of accurate personal information may impact one's private life. The example in this respect is the accurate registration of one's religion in the Dutch population registers. In WWII, the Nazis used the registration to efficiently find Jewish people.

5.8.2 Inaccurate information

For national security and law enforcement purposes, it is of evidential importance that the processed core information is accurate (see Buruma 2001, p. 137). The accuracy of data in private databases seems to be a major problem (Buruma 2001, p. 137). Causes for the errors and noise in the databases are manifold. Data entry by unqualified personnel, no verification of a single source, old data, and inaccuracies because of identity theft, among others, contribute to inaccurate information in these databases. White (2007, p.18) noted:

> "One digit misread, and the wrong license plate goes into the database. Facial recognition software misreads a feature, and evidence that you were somewhere you have never been enters your profile. The Congressional Research Service has estimated that under a government data-mining scheme, a conservative estimate of ratio of false terrorist suspects to actual terrorist suspects found by the system to be 200 to 1". (referring to Belasco 2003, p. 16).

Thus, for every terrorist identified, some 200 other suspects would have to be investigated (Belasco 2003, p. 16).

Mell (1996) notes that verification of information in database records "typically involves comparing the record to other records, not consultation with the individual who is the subject of the record." [] Quality control of data in security and intelligence agencies is difficult since "individuals often do not know of the existence of many of the dossiers about them, or what is in those they do know to exist, there is usually no process to challenge the accuracy of fact, opinion, or rumor the files contain" (Westin 1967, p. 160). And even if they do know, they may be confronted with a system that is unlikely to be willing to change the 'facts' in the database based on the information provided by the individual concerned (see O'Harrow Jr. 2005 for multiple examples). In other words: There's no way of getting off the list (O'Harrow Jr. 2005, p.141). One may conclude that the assumed 325.000 people on the terrorism suspect list in the US will be confronted with this list for the rest of their lives (see Pincus et al 2006).

Also with respect to location information, inaccuracies may exist. The collection of location information always comes with inaccuracies. A map, or other location information is a model of the real world. A simple representation, which serves primarily the purpose for which the data was collected. Inaccuracies may be the result of many elements in the data process. It may be because we are trying to fit a 3D world to a 2D map, with scale, or with other decisions in the location information processing process. For example, a choice may be made to collect only a limited, task specific, type of location information; only physical objects higher than 25 metres. Or only the location information in the direct environment of water. Further, the cartographer may choose for a specific representation, which may not be understood by others in the same way.

Before in chapter 4, we mentioned an interpretation error of location information when someone was visiting the supermarket instead of a coffee shop just below the supermarket. But not only in the 3D and 2D differences wrong conclusions may be drawn. For example, the 2D location information of cell-phones has an approximate accuracy of 100 metres in urban areas, and in rural areas it may several kilometers. With such inaccuracies, it will be very difficult to conclude that someone was at a specific place at a certain time. Positioning data may then be useful to assume some data, but other sources or means need to be used to be certain about the cell-phone data. Thus data that a cell-phone has communicated close to location X may be useful as indication of the location of this cell-phone, no more and no less.

Similar cases are known from stolen cell-phones, which were used in a criminal act, resulting in the by mistake arrest of the subscriber, the assumed user, of the cell-phone (see, for example, Logtenberg 2008).

Also timeliness of location information is important in this respect. One may remember the incident in Serbia where the Chinese Embassy was mistakenly bombed because of outdated location information (see Ponce 1999).

5.8.3 Data Doubling

The above results in a situation of data doubling. Data doubling is the term used for one's virtual data double, a decorporealized body stored in a variety of databases and reassembled somewhere else for various purposes (see IPTS 2003, 176). As a consequence, who am I is typically a question the data mining companies can better answer than the individual concerned.

> *"They know things about you, you didn't know yourself"*
> (O'Harrow 2005)

The data mining capacity has resulted in a situation where "the ratio of what individuals know about themselves (or are capable of knowing) versus what outsiders and experts can know about them has shifted away from the individual" (Marx 1998, p.172). For example, O'Harrow Jr. (2005, p.300) notices:

> "It takes less and less effort each year to know what each of us is about. When we were at the coffee shop and where we went in our cars. What we wrote online, who we spoke to on the phone, the names of our friends and their friends and all the people they know. When we rode the subway, the candidates we supported, the books we read, the drugs we took, what we had for dinner, how we like our sex. More than ever before, the details about our lives are no longer our own."

"The dangerous aspect of such [dataveillance] dossiers is that the raw facts about individuals take on added weight because they are part of an "official file" complied by an investigative agency" (Westin 1967, p.160); the recorded personal information achieves more credence than the individual involved (Mell 1996). One may wonder until when we are allowed to overrule our own digital shadow (Boutellier et al. 2005, p.29). These developments need to be carefully considered because accurate or not, data is forever (O'Harrow Jr. 2005, p.138).

5.8.4 Competence of intelligence services

Intelligence services use information of others, but also collect information themselves. Also information from intelligence services may have unintended secondary uses. In the Netherlands, in recent years in several occasions memory sticks, and computers with sensitive information have been found on the street or stolen from intelligence and law enforcement officers. In the US there have been many instances where intelligence and law enforcement officers have misused their access to sensitive information, for example to sell these records. More painful are the white-collar crimes, or cooperative moves. These "seem particularly characteristic of control systems where agents are poorly motivated or indifferent, feel fatigued, and are under-rewarded. They may also sympathize with those they are to surveil" (Marx 2002, p.383; Levi et al. 2004, p.214): "There isn't anybody, anywhere in law enforcement, that doesn't check people out. If they say they don't I'd stake you a hundred that they're lying" (O'Harrow 2005 citing a former sheriff' deputy, p. 274).
In addition, at the end of 2006 in the UK terrorists were intercepted with a bomb made of liquids. Since then all airports in Europe are focusing on liquid bombs. In 2007, the author (BVL) was stopped at the gate at Schiphol International Airport for having a bottle in his hand luggage. The bottle was confiscated, but surprisingly his razor was not noticed or taken.
Another example that does not contribute to the confidence of society in intelligence services is found in the way aerial imagery is being addressed, for example in GoogleEarth. RAND has found in 2004 that national security has only for a very limited number of data

sets a reasonable risk (RAND 2004). However, in the Netherlands all military buildings, including those of the national security and intelligence services are not visible on GoogleEarth. Non-visible implies that the military building is covered with fancy colours as figure 1 shows. In this specific example the information is also outdated and one may wonder how effective such 'masking' is. There are now even discussion groups trying to identify all masked objects. As a consequence, one may wonder how effective our national security officials are in protecting our national security. Still, the Minsitry of Defence is investigating the extent to which MS VirtualEarth, which does show certain military buildings, is threatening national security (Leeuwarder Courant 2008).

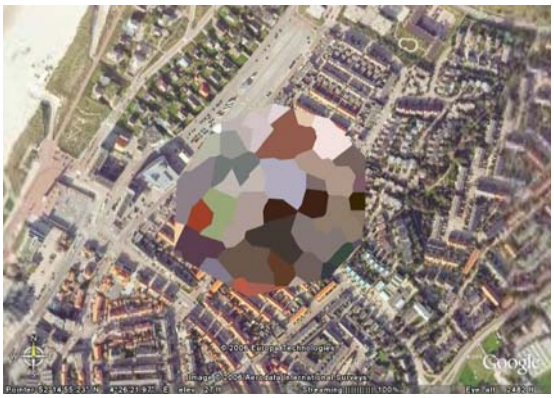


Figure 5.1: What UFO has landed in Noordwijk aan Zee? Defensie Pijpleiding Organisatie is reeds verhuisd naar Den Haag (website Nu; see also website Marketingfacts for an overview of scrambled places on GoogleEarth).

Capacity of intelligence services

Tracking the 147 potential terrorist in the example presented before, based on one single profile will be a challenging task for the Dutch intelligence service and its' 1100 employees. Do we leave it at these 147, or are there other profiles that are assessed to be as critical? If the current focus is on one profile, does this imply that other profiles are completely ignored? (cf. O'Harrow 2005, p.242). Are native Dutch citizens, Catholic, middle class, with three daughters by definition innocent and are not considered by intelligence services until one of them decides to shoot a politician? In other words how stable are the profiles of threatening individuals or groups and how often do these need to be changed?

5.9 Just action to protect national security interests

The protection of the national security aims to protect the principles underlying our democratic societies. The protection of national security is necessary and may invade privacy rights. Surveillance may be an important factor in protecting national security. One may argue that in general, surveillance does not raise security. Modern societies are vulnerable. It is impossible to foresee, or prevent terrorist attacks such as 9-11 (Peissl 2002). Especially when terrorist are willing to risk their lives anyway (Peissl 2002). But, on August 10, 2006, MI5 has informed us to disrupt a plot aiming at bombing several airplanes. Twenty-one suspects were arrested and it is likely that a new tragedy was prevented.

However, we should not loose ourselves in the tempting thoughts that more information is always better and that it is possible to eliminate crime. Privacy-invading technologies are not necessarily increasing the effectiveness or success of the national security and intelligence services. Technology has its limitations and these should be considered when discussing and

deciding on the means to use. "A more realistic hope – and one that is less destructive of human right values – is that crime levels can be reduced to pose a less serious threat to the economy and society at large" (Levi and Wall 2004, p.220). Often, it is a matter of linking the appropriate and already available information.
Although some suggest that the 'Surveillance Society' is already with us (DPWP, 2006, p.1; Wood et al. 2006; O'Harrow 2005), surveillance seems to be relatively under control in Europe. This may explain why public trust in their governments that the privacy intrusions are for necessary and proportionate purposes are paramount (DPWP 2006, p.3). If public confidence is lost or severely damaged, it may be difficult if not impossible to regain (DPWP 2006, p.3). Therefore, it is critical that interferences with the private life for the protection of national security are such that the principles developed by international legislation are being adhered to and enforced (see chapter 2). This implies that in creating this surveillance assemblage one should at least take care of proper data processing measures as required by Article 5 of the Council of Europe Convention no. 108. This includes clear authorization for access to the data (see Westin 1967, p.158), secure data communication, and use of accepted data quality control procedures. This applies both to the data processing of old data and to the processing of real-time data such as location data from a cell-phone. In addition, "through offering high quality documentary evidence and audit trials, the new surveillance may enhance due process, fairness and legitimacy" (Marx 2002, p.22). Adequate data processing mechanisms with both internal checks and periodic checks from independent authorities are required. But this is difficult since the data processing concerns "secret determination based on a secret analysis based on a secret category of information" (O'Harrow Jr. citing Senator Sobel, 2005, p.237; ROB 2005, p.40).
However, only with sufficient safeguards in place, trust in the operations of intelligences services will be created. Misuse of the concept of national security to address other issues and misuse of the execution of a national security task need to be prevented to the greatest extent possible.
Key question remains when, how, how long and who decides and controls when and how? Thus, how to balance privacy needs with national security needs?

5.10 Conclusion

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. National security is an extremely flexible notion, however. It is difficult to assess whether something or someone is a threat to the national security. The interpretation of the concept may be different from society to society, culture to culture and may change throughout time.
Many means may be used to protect the national security. Physical, and data surveillance are among these. There are many examples available that show that these means can be effective. However, there are many aspects that need to be taken into account in using these means (e.g., accuracy of processed information, interpretation of the data, competence of intelligence services).
Decisions based on the processed data may have a great impact on individuals and eventually on society. Sufficient safeguards should be in place to ensure to the greatest extent possible that it is only national security that is protected, not another interest, and that the use of the means protecting national security are strictly limited to what is listed in the task to which the means were assigned.

6 The ambivalent role of (location) technology

6.1 Introduction

Technology has an ambivalent role in location privacy of mobile devices. On the one hand technology may diminish location privacy and enhance national security through the possibility to trace and track mobile devices. On the other hand, technology also allows users to choose through privacy enhancing technologies to not to be traced or tracked.
In this chapter, attention will be given to the state-of-the-art technological possibilities related to both the tracing and tracking of the mobile devices, the so-called privacy-invading technologies (PIT), as well as to technologies preventing the tracking or tracing; the privacy enhancing technologies (PET). Finally, new technological developments will be addressed to account for emerging threats and future solutions.

6.2 Developments in society and technology

Western societies can be characterized as information societies; information is driving the economy and society. Key for the development of the information society is its information infrastructure. One of the most significant benefits of an information infrastructure is that it promotes the minimisation of duplicate information collection. "By facilitating information sharing and to allow for information integration, the value of existing information resources is maximised. The time, effort and resources previously spent on the collection of the same or similar information may now be used to collect new information or to create new innovative products. By reducing duplication and facilitating integration and development of new and innovative applications, [information infrastructures] can produce significant human and resource savings and returns" (after Chan et al. 2001, p. 65). In addition, information infrastructures may allow users to respond more effective to demands from society, for example, through 24/7 available services (see King and Kraemer 1995, p. 14). This holds in particular when the combined use of location and administrative data is concerned. It may promote economic development and make countries highly competitive.

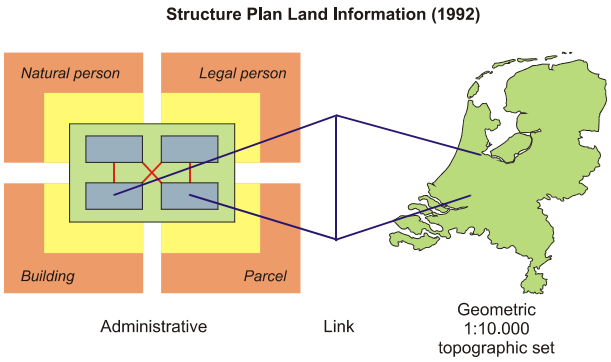


Figure 6.1: Optimised geographic information infrastructure: ubiquitous linking of key data sets (Ravi 1992)

It is foreseen that citizens will be come more acquainted with modern technology, more aware of the benefits of location information, and more demanding of mobile services, and as a result they will require more detailed and more enhanced services (Smith et al. 2003). The value-added services of GoogleEarth and MS VirtualEarth are examples of services that increasingly include highly detailed satellite imagery with vector datasets of road centrelines and, if available, more detailed information such as buildings. It is probably only a matter of time before citizens start requiring detailed information for uses they now request irregularly but will soon use on a daily basis. The level of detail and currency that users will require is likely to be greater than current information timeliness (Van Loenen 2006).
Modern technology allows for faster, more accurate, and more current information collection, speedy dissemination, and searches and analyses by geographic unit, making it extremely useful for geographic management and planning, for example disaster management purposes. The new information resources can also be used to ensure the public safety, without which privacy itself becomes a nightmare isolation (Westin 1967, p.60). Although the increased interoperability of these locationisers serves many users well, it potentially allows for the ubiquitous surveillance of objects including individuals.
Traditional location technology such as theodolites, GPS-receivers, photogrammetry and remote sensing is now expanded with high sensitive GPS receiver chips, RFID technology, and ubiquitous telecommunications or IT networks. Even if one chooses not to use the internet, or cell-phones, in the future the RFID tag of your sweater, laptop, PDA, watch, and other mobile objects combined with WiFi (wireless fidelity) or UWB (ultra wideband) networks may reveal your location.

"*Recent advances in digital networking, data storage, capacity and processing power have enabled previously unimaginable levels of interconnectivity, aggregation, and real-time analysis of a wide array of personal information*"
(Zimmer 2006, p.204)

Due to these technological developments, an increasing amount of administrative and geographical information is available through an increasing number of channels. In the 1990s, it has been assessed that the average Dutchmen is registered in approximately 900 registrations. Previously, these were all unique datasets that were not linked to each other (see figure 6.2). However, currently it is at least in theory possible to link any digital data set with any other.

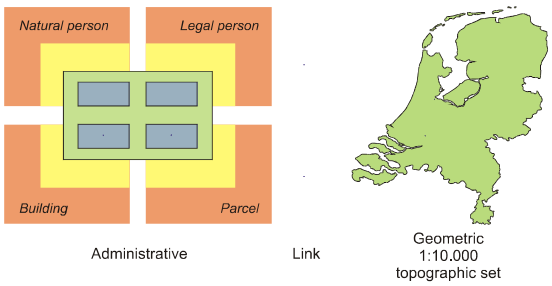


Figure 6.2: Privacy optimised: no linking between datasets (figure based on Ravi 1992)

Together, the acquired data allows for inferred assumptions about individual's income, health, lifestyle, buying habits, travel behaviour, and social network, amongst others (see EU 2005, p.6; Wood et al. 2006). Through developments in artificial intelligence the 'individual' becomes more transparent than ever before (see O'Harrow Jr., 2005, p.265; Clarke 2001, p.219). This so-called dataveillance may threaten privacy. One consequence is that "Companies could now know who you were the instant you called" (O'Harrow Jr. 2005, p.42) and consequently address you with an appropriate attitude that fits your profile.
Especially the secondary use of these personal data, which were beyond the purposes for which they were designed are considered a major threat to the privacy (see Levi and Wall 2004, p.213; O'Harrow Jr. 2005, p.291).

6.3 Privacy invading technology

> *"Forget dropping a coin into a parking meter or using a pay phone discreetly on the street. Those days are slipping by. The most simple, anonymous transactions are now becoming datapoints on the vast and growing matrix of each of our lives. The fact that you did something at a particular time [] will be recorded and will never go away until the last hard drive is destroyed."*
> (O'Harrow Jr. 2005, p.291)

Already in 1967, Westin acknowledged that "In the field of locating individuals and following their movements, signal-transmitter "tags" promise to become steadily more powerful and less expensive. [] such tags will become available in much smaller sizes, increasing still further the possibilities of secreting them in an individual's clothing or his personal and professional accessories" (Westin 1967, p.85) Westin even considers permanent implacements of "tagging" devices on or in the body. He predicted that "Signaling devices have been produced already (and will become smaller and more powerful) by which persons within a building or miles away can be buzzed to let them know that they are wanted or that they should call in: these systems might also be used for locating individuals" (Westin 1967, p.88-89). Anno 2008, Westin's future has become reality. Baja Beach club members pay through their implanted tags, the logistics sector is heavily relying on RFID technology, and cell-phone and IT networks have become the signalling devices locating individuals.
Several means exist to track people down. These privacy invasive technologies (PITs) may track and trace people either real-time or ex-post. Here, we distinguish devices actively revealing their location and devices passively providing their location.

6.3.1 Devices that *actively* reveal location information

The most promising or threatening devices that allows for real-time tracking are devices that actively provide information on their location. Cell-phones, and wireless personal area networks (PANs) are among those. Without claiming to be exhaustive, we discuss cell-phones, wireless networks, and active RFID tags.

Cell-phones[15]

The worldwide standard of cell-phone the GSM network (Global System for Mobile communications, originally from Groupe Spécial Mobile), consist of three components (Scourias 1997, see figure 6.1):

- Mobile station (the cell-phone)
- Base station subsystem
- Network subsystem

The mobile station has three key components. It has a unique International Mobile Equipment Identity (IMEI) attached to it. Further, a SIM card is necessary to use the cell-phone. The SIM card contains a unique International Mobile Subscriber Identity (IMSI). The telecom provider attaches the IMSI code to a phone number (the Mobile Station ISDN). The IMSI code can be linked to the name and address of the subscriber and will identify the subscriber. For pre-paid phones this link may not exist, however. Finally, the user of the mobile station can be distinguished. The user is not necessarily synonym for the subscriber. Voice-recognition technology or experiences may be used to link the voices through the cell-phone to an individual.

The average reach of a GSM device is approximately 5 kilometre. Therefore, for full coverage of an larger area it is required that telecommunication towers are available every other 5 kilometre. At least because the signal strength is heavily interfered with constructions such as buildings. In densely populated areas, the towers are more likely to be found every other kilometre. In theory, each tower covers a roughly circular area: the cell. The shape of the cell may deviate due to constructions, and other choices to serve an area in the most economic way. Each of these telecommunication towers, the so-called Base Transceiver Stations (BTS), are managed by a Base Station Controller (BSC). A BSC manages the connection between one or more BTSs, which channels are assigned to the cell-phone, the handing over of content, and at what strength the mobile device and the BTS sends. The BSC is the connection between the BTS and the Mobile services Switching Centre (MSC).
Based on the strength of the signal from a phone at multiple antennas the MSC decides which BTS is being used for a phone call. It uses several databases for identifying the mobile device, its subscriber, entitlements to specific services, and keeps track of the location of the device. As the cell-phone moves, the base station receiving the strongest signal changes, and the network "hands off" the call from one base station to another (website IEEE).

The MSC consists of four databases:

- Home Location Register (HLR);
- Visitor Location Register (VLR);
- Equipment Identity Register (EIR);
- Authentication Center (AuC).

The HLR consists of administrative data such as the name of each subscriber registered in the corresponding GSM network, together with the current location of the cell-phone. The HLR has:

- IMSI;
- MSISDN (telephone number);
- GSM services requested or given;
- Current location of the device (through VLR);

[15] Based on Scourias 1997

- Service subscription data.

The VLR is a temporary database of subscribers who have roamed into the particular area which it serves. Each BTS is served by one VLR. In the VLR the following data is being stored:

- IMSI;
- Authentication data;
- MSISDN;
- Services allowed to be accessed by the device;
- HLR address of the subscriber.

The EIR maintains a list of IMEIs in the network and categorises the IMEIs with white (it is okay to connect to the network), grey (the device is under observation by the network for possible problems) or black-listed (device is not connected to the network; e.g., the device is reported stolen or GSM type is interoperable with the network).

The AuC has a copy of the secret key of the SIM card. This code is being used for identification and encryption of the signal.

How does it work?
All BTS send periodically a unique signal to let cell-phones know where the BTS is. When a cell-phone is switched on, it searches and registers the signals of a maximum of (the strongest signals) 6 BTS stations. Every second, this list will be send to an available BTS. The BTS sends this list to the BSC, which sends it to the MSC. The MSC decides which BTS to use. In the VRL database the location of the cell-phone is registered and through the VRL the HRL is informed that the device has arrived in a particular area covered by that VLR.
When a device moves from one BTS to another a location update message is sent to the (new) MSC/VLR. The MSC/ VLR sends the location information to the subscriber's HLR. If the subscriber is entitled to the service, the HLR sends a subset of the subscriber's information (needed for call control) to this MSC/VLR. It also sends a message to the old MSC/VLR to cancel the registration.
The VLR keeps track where the device is within the VLR area when no call is ongoing (website mediatheek).

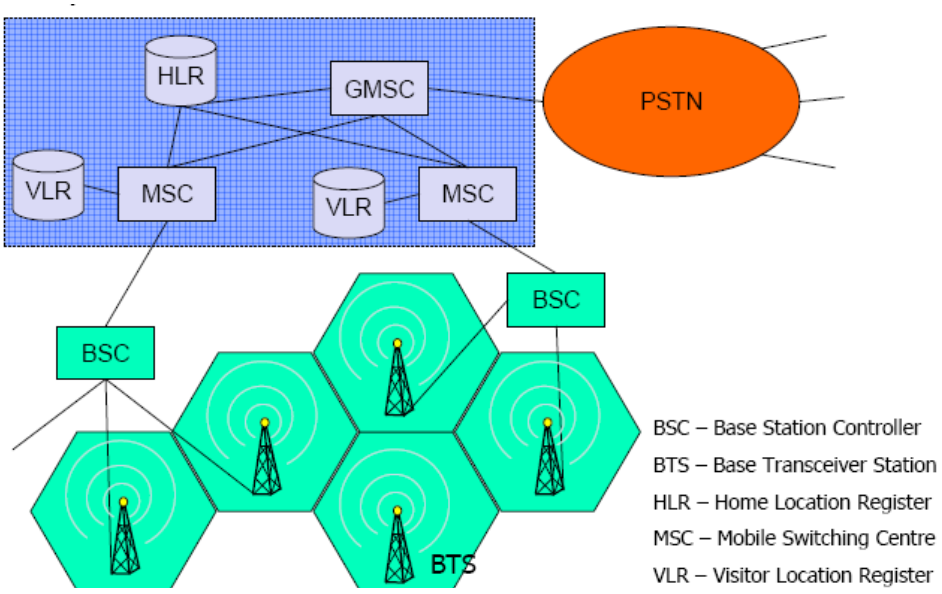


Figure 6-3 Overview of the telephony network (Lo 2007)

Thus, in order to set up and maintain a connection the network needs location data, and when switching between networks the need for processing location data is evident. Network operators by technical necessity have to exchange location data to be able to provide the telecommunication service (Penders 2004, p.255); the processing of location data is a prerequisite for telecommunication services. Differences in signal strength of received BTSs, observed time differences between synchronised signals that a cell-phone receives, or time differences with which the different BTSs receive the signal of the cell-phone may be used to calculate the location of the cell-phone more detailed (see Van Wijngaarden 2001 cited in Lips et al. 2004, p.32). This calculation, so-called triladation, establishes a more detailed location of an object than necessary for enabling communication through the device. Third generation GSM will provide location information at an even finer granularity (see also Cvrcek et al. 2006, p. 109; Matyas and Kumpost 2007).
Also other creative ways to arrive at a more accurate location than the regular BTS-data exist. For example, for every location, the BTS-data (which are the 6 'strongest' towers received at this point) can be processed and linked to GPS data. Each unique location (with a unique combination of 6 signals and strength) is pinpointed to coordinates. In this way a ubiquitous network may be developed that links with high accuracy BTS signals to a location. Devices may be equipped with a chip that actively provides this information to others including the telecom provider. An example of such system is found in livecontacts (website livecontacts).

Further, 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 et al. 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* referred to by Koops 2006, p.18; Bundestag 2005). This may, however, not be without risk since a message may arrive at the cell phone indicating that it has missed a call or message. Another option may be to activate the microphone in the cell-phone and track the cell-phone down (Logtenberg 2008).

Accuracy of location

The accuracy of the location of the cell-phone varies per situation. Generally, in urban areas an accuracy of 100 meter may be feasible, while in rural areas an accuracy of several kilometres is possible (see also Miedema and Post 2006, p.13). Some claim that an accuracy of several metres can be achieved (Van de Pol 2006, p.141; Odell 2005), but this is very unlikely without the use of additional technologies such as GPS. The way the cell-phone network works does not allow for absolute guarantees that the cell-phone uses the nearest BTS. It may very well be that this nearest BTS has reached its capacity, or for other reasons is unavailable and directs the call to another BTS. This may be a BTS several kilometres away from the location of the cell-phone.

For communications through the data channel (e.g., SMS, MMS) the nearest BTS is being used.

IMSI-catcher

In the context of this resarch, also the IMSI-catcher should be mentioned. An IMSI-catcher measures the signal strength of received BTSs and pretends to be a BTS. Cellphones in the surroundings of the IMSI-catcher recognise the IMSI catcher as a BTS and connect to this BTS since it provides the strongest signal. With the connection the cellphone provides its IMSI number. Thus, the IMSI-catcher allows for revealing the IMSI of a cellphone, but it also allows to track a cellphone down to the direct surroundings of the IMSI-catcher.

Satellite phones

Satellite phones communicate through the use of satellites. The current location characteristics are such that this technology is not considered to be as privacy sensitive as other locating technologies. Neither is the use, with respect to tracking and tracing, as useful for national security purposes. Currently, the positioning accuracy is claimed to vary between 300 to 10,000 metres (see website REI; website Globalstar; website Space). Others holds that the position of a satellite phone can be determined within a 150 kilometres radius (Clarke 2001, p.214). One must be outside to have it working and compared to regular cell-phones they are expensive.

Active RFID tags

Radio Frequency identification technology (RFID) or infrastructure consist of a tag (i.e. a microchip) and a reader. The tag consists of an electronic circuit that stores data and an antenna, which communicates the data via radio waves. The reader possesses an antenna and a demodulator, which translates the incoming analogue information from the radio link into digital data. The digital information can then be processed by a computer (EU 2005, p.3). The tags can be active or passive.

"Active" tags have their own battery. They either broadcast their information without being interrogated by the reader, or stay quiet until triggered by a reader (EU 2005, p.3). "Active tags transmit at higher power levels than passive tags, allowing them to be more effective in "RF challenged" environments like water (including humans/cattle, which are mostly water), metal (shipping containers, vehicles), or at longer distances." (www.wikipedia.org). Active

tags have a relatively large broadcast range (up to 100m) and are generally used when the location of the tag is more important than the data stored on it (Lockton et al. 2006).

Figure 6-4: RFID tags revealing information to the environment

Wireless personal/ local area networks

Modern technological networks potentially allow for the ubiquitous surveillance of mobile devices. The ubiquitous identification may become reality with the rapid development and implementation of Wireless local area networks (WLAN). Examples of 'Wireless Positioning Systems (WPS)' are WiFi ('Wireless Fidelity') and UWB (Ultra wideband). WPS relies on wireless Internet access points and uses them to determine the position of mobile WiFi-enabled devices, such as PDAs, cell-phones and laptops (Luccio 2006).

WiFi is a term for certain types of wireless local area networks (WLAN), providing access to the Internet. Ultra wideband (UWB) is wireless technology that allows data to be transmitted over several radiofrequencies at the same time with great speed (see Delta 27 2006, p.7). It has a range of up to 100 meters (Delta 2008, nr. 3, p.16). Both enable or may enable the linkage of the identification of devices or tags to a certain location in the network. Gruteser et al. (2004, p.17) notices that the density of WLAN access points in densely populated areas makes it difficult to use a WLAN network without being detected by other parties.

A wireless personal area network (WPAN) can also be made possible with network technologies such as IrDA and Bluetooth (wikipedia.org). Bluetooth provides a way to connect and exchange information between devices such as personal digital assistants (PDAs), mobile phones, laptops, PCs, printers, digital cameras and video game consoles via a secure, globally unlicensed short-range radio frequency (wikipedia.org). It is part of the short-term wireless connectivity technology. Devices hosting Bluetooth are relatively smart compared to RFID tags (Wong et al., 2005, p.182). The Bluetooth Device Address (BD_ADDR) may reveal an individuals location. Especially if a cluster of BD_ADDR is detected it is highly probable that the individual is nearby (Wong et al. 2005, p.177). Bluetooth has a range of 1 to 100 meter (wikipedia.org).

Since WiFi routers are plentiful and still rapidly increasing in number and are created for enabling wireless internet access, it is relatively inexpensive to hook up this system to the tra-

ditional positioning systems and create a ubiquitous surveillance system, previously assessed to be too costly to be implemented.
These technologies are now readily available, and with the access point of the WiFi router, or Bluetooth-connections known, a user of these becomes easy to identify and the possibility arises to use the internet to track the location of these mobile devices.

Hybrid systems
GPS and WPS equals XPS. In April 2006, *Luccio* reported that at least one company is working on the integration of GPS and WPS in one positioning system. 150 drivers are collecting WiFi access points detected and the strengths of their signals at a certain position. It is stated that in any urban area between 3 and 15 networks for any point can be 'heard' and in 95 percent of the time at least two (Luccio 2006). The accuracy has increased from 20-50 meters in 2006 to 10 meters for 85% of the positioning in 2007 (Luccio 2007). The meter level is currently beyond the system.
According to Luccio, the WiFi access points stay fixed for at least 12 months. In 2007, the company SiRF and Skyhook had 15,000,000 access point in their database covering 70% of the US population and 60% of Canadian population (Luccio 2007). The system can tell in real time that a certain number of people are on line in a certain area at a certain time. Although possible, the company does not intend to track people.

6.3.2 Devices that *passively* reveal location information

Ad hoc tracking with a potential for real-time tracking: Radio Frequency Identification Tags (RFID)

Other locationising devices allow for tracking of objects or subjects, but only if the device is within the reach of the receiver. Those include passive RFID, license plate recognition.

RFID
Radio Frequency IDentification (RFID) consists of two main components: the RFID tag and a reader. The tag contains a transponder with a digital memory chip that is given a unique electronic product code. When an RFID tag passes through the reader's electromagnetic zone, it detects the reader's activation signal. The reader decodes the data encoded in the tag's integrated circuit and the data is passed to the host computer (EU 2005, p.3; website wikipedia 2006, 1 October, www.wikipedia.org).
The data transmitted by the tag may include all kinds of information including personal information, or specifics about the product such as price, colour, date of purchase, etc. "[] As of 2006, the smallest such devices measured 0.15 mm × 0.15 mm, and are thinner than a sheet of paper (7.5 micrometers).[] The lowest cost EPC RFID tags [] are available today at a price of 5 cents each. Passive tags have practical read distances ranging from about 10 cm up to a few meters depending on the chosen radio frequency and antenna design/size. [] Passive RFID tags do not require batteries and have an unlimited life span. [] (www.wikipedia.org; EU 2005, p.3). RFID tags have been described as real-world "cookies" linked to us, sending back information about everywhere we go (O'Harrow Jr. 2005, p.289).
RFID is being used worldwide for controlling access to buildings, identifying cattle, anti-theft systems, and automated payment at toll roads (EPC.NL 2005, p.14). Also human beings may be equipped with RFID tags. In the entertainment park Legoland children may be equipped with an RFID bracelet that can be tracked anywhere within the park's boundaries (website silicon). More extreme, in the Baja Beach Club, the VIP lounges are providing the

implantation of a tag in own body to check in and to pay drinks (ECP.NL 2005, p.12). Members of the club consider this a great service. But what happens when the tag identification becomes ubiquitous and what may happen if the item containing a RFID (say a woolly jumper) has been sold, stolen, borrowed, given away? (IPTS 2003, 175).
RFID may not yet be a significant threat to the privacy because the independent RFID systems are not fully interoperable. ECP.NL doubts whether the private sector is willing to create such dense systems that devices can be tracked and traced on a continuous basis (ECP.NL 2005, p.35). However, EPCglobal Inc. is working on the creation of 'Electronic Product Codes' (EPC), which will identify individual items. The EPC Global Network is progressing towards a global standard to connect servers with EPC information through EPC information services (EPCIS) (EU 2005, p.13).

License plate recognition and other technologies
Another example of ad hoc tracking are surveillance systems that coverge optical information about car number plates with driver databases are found in the use of roadside speed cameras (IPTS 2003, p.169; Clarke 2001, p.216). Also red-light cameras are in this category (*flitspalen*) (see White 2003, p. 16), and traffic management camera's. Although the purpose of these technologies are satisfied once a penalty or fee has been processed, the location data might be stored longer than necessary.
White (2003, p. 16) recognised another category: the flexible tracking devices such as credit cards, loyalty cards and other devices that with permission of the user may have the unintended consequence of revealing a user's location at a certain time. In this category also toll booth information fits.

6.3.3 Ex-post continuous tracking: Navigation satellites

Navigation satellites typically send one-way information to receivers. The satellites do not receive data from the receiver. Based on the information from the satellites, the receiver can determine its approximate position. Currently this can be up to the meter level. Examples of navigation satellites are Global Positioning System (GPS, US), Global Navigation Satellite System (GLONASS, Russia), Beidou Navigation System (China), and the planned Indian Regional Navigational Satellite System (IRNSS, India) and Galileo positioning system (EU).
Although GPS-receivers do not send information, they may be incorporated in other devices that have the ability to send. These may also send GPS information, for example, to better take advantage of a LBS. These so-called 'active GPS' allow for the continuous tracking of devices. For example Acme, a US-based car rental company, rents its cars with a computer, a transmitter, and a back-end server that enabled Acme to watch the car's progress on a Web page. In one instance, they withdrew the penalties assessed for three speeding violations in three states (O'Harrow Jr. 2005, p.292).

6.4 Privacy enhancing strategies

A wide range of privacy enhancing technologies are available. However, since the availability of the location information is a prerequisite for using the functionality of 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 intelligence services they may not. Thus, relying on technology alone to protect individual's privacy may be insufficient.
There are several other ways to circumvent surveillance (technologies). There are psychological ways of achieving privacy as well as physical arrangements (Westin 1967, p. 12). A satisfy-

ing stage of privacy may be reached with behavioural techniques provided by Marx (2003). He has identified eleven behavioural techniques of neutralizing the collection of personal information (see also section 5.8).

The first technique, the discovery mode, is to find out if surveillance is in operation and where it is. This may well compare with the anti-radar 'fuzz buster' that warns when a police radar is in use (see also Westin 1967, p.82).

The second technique, the avoidance mode, involves withdrawal. Examples may be avoiding supermarkets with frequent shopper cards, pay in cash, making calls from a pay phone. Another form of avoidance is not raising the red flag. "Knowing that certain profiles or crossing certain thresholds will trigger surveillance or at least suspicion, individuals stop short of this or avoid triggering characteristics" (example of bank deposits under $10,000). Levi and Wall (2004, p.214) go further in this opting out strategy. They foresee a complete new underground world of those hiding from the state.

In the third technique, piggybacking moves, a control is evaded or information protected by accompanying or being attached to a legitimate object or subject (example of driving/walking quickly behind a person with legitimate access).

Switching moves involves the transfer of an authentic result to someone or some thing to which it does not apply (example substitute test takes, 'cut off the thumb' case).

Distorting moves manipulate the surveillance process such that the technical data do not mean what they appear to say (cf. Westin 1967, p.82).

The sixth technique, blocking moves, seeks to physically block access to the communication or to render it unusable (example playing loud music, whispering, metallic shield in bag to block sensors, encryption of communication) (cf. Westin 1967, p.82).

Masking involves blocking, but it goes beyond it to involve deception with respect to the identity, status, and/ or location of the person or material of surveillance interest (false license plate, false ID).

The eighth move, breaking moves, render the device inoperable (disabling phone lines, spray painting a monitor).

Refuse moves ignore the surveillance (example I do not have a phone, social security number, income, house).

The tenth technique, cooperative moves, involve the white-collar crime. These "seem particularly characteristic of control systems where agents are poorly motivated or indifferent, feel fatigued, and are under-rewarded. They may also sympathize with those they are to surveil" (Marx 2002, p.383). Examples of this 'social engineering' (Levi and Wall 2004, p.214) are found in the Hofstad group and the AIVD interpreter case.

Finally, Marx provides the counter-surveillance move, surveiling those who are doing the surveillance: private wire-tapping or bugging conversations of law-enforcement officials (Westin 1967, p.116).

One of the biggest threats to the success of surveillance technologies, however, are strategies that can be described as 'to live a life as anyone' in addition to avoiding identifying technologies. These *privacy enhancing strategies* may be to pay in cash, avoid the internet, use false IDs, using other people's artificial numbers, etc. These individuals typically 'opt out' and keeping out of the system and therefore maintaining invisible (see also IPTS 2003, 137). However, this implies opting out of the opportunities of information societies. It is unlikely that many are willing doing so.

Others suggest that everybody providing everything that is known to them and about them online is the best way to preserve privacy. It is suggested that information technology cannot cope with the huge amounts of personal data and the complete state of informational privacy may be reached (Thompson 2007). However, this implies that also other critical functions of society, which are building on IT, will also fail.

For those that cannot do without the temptations of the information society may use *privacy enhancing technologies* to avoid surveillance. Anonymizers and encryption are typical PETs.

Privacy enhancing technologies (PETs)
In assessing Privacy enhancing technologies one should distinguish between devices that users need for their own functioning in daily life such as cell-phones and PDA's, and devices that users do not need or even do not know about them such as RFIDs.

Concerning RFID, the easiest protection is to wrap the RFID-chip in aluminium foil (Lockton et al. 2005/6). This would be difficult if the tag is attached to your sweater or jeans, however. More advanced options are on the user control side to kill these tags upon purchase of the attached item, or its ID can be re-encrypted by an external agency (Wong et al. 2005, p.176). Another supplier driven option may be that the tag is changing its ID on every query (Henrici et al. 2004, p.221). The RFID tag can also be equipped with a "Hash-Lock" which ensures through cryptography that the information on the tag is only revealed to the receiver if the reader has the right key to read the tag (Henrici et al. 2004, p.220).

For mobile devices one think of a Faraday cage which prevents radio waves entering or leaving ensuring no surveillance, but also disabling any communications (see Wheeler 2004). If one still wants to communicate one may use an information diffusion approach to scatter the user's location information to confuse the attacker (Lee et al. 2005, p.1007), or use frequently changing pseudonyms (Wong et al. 2005, p.83). Use of encrypted and anonymously purchased mobile phone communications between offenders make both them and their content difficult to trace (IPTS 2003, 180).
Although these PETs do protect the content of the communication, this excludes the location of the device. Since the availability of the location information is a prerequisite for using the functionality of 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 intelligence services they may not.
In addition, encrypted data can be deciphered and anonymous identities can be de-anonymized, even when they are in the hands of trusted third parties/ intermediaries. Often those who developed these deciphering technologies are working for or co-operating with intelligence services. There are no guarantees that encrypted or anonymized data will remain forever unknown, or that in special instances (e.g., to protect national security) the PET will be 'de-activated' (cf. Clarke, 2001, p.213; see also Gruteser et al. 2004, p.15, Lee et al. 2005, p.1009).
More specific, those using these PETs may be likely to be subject to surveillance because of their suspicious behaviour of using PETs. What do they have to hide?

6.5 Conclusions

In this chapter we explored the state of the art technological opportunities in determining the location of mobile devices. Depending on the density of BTS and or WiFi transmitters the position of a mobile device can be determined varying from a few kilometres to the 100 meter level. In the future, the meter level will be feasible. Devices using active GPS, i.e. sending GPS information, can be determined at improved levels of detail. These developments in technology are expected to result in hybrid systems that incorporate a location identifying component. We foresee developments towards the integration of location information avail-

able within WiFi networks, RFID networks, cell-phone networks, together with active GPS in mobile devices. Although we might be decades from full integration of these networks, these potentially allow the permanent identification of individuals within a range of a few meters. These privacy invading technologies are likely to extend the abilities of secret intelligence to better address national security.
A wide range of privacy enhancing technologies are available. However, since the availability of the location information is a prerequisite for using the functionality of 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 intelligence services they may not. Thus, relying on technology alone to protect individual's privacy may be insufficient.
In theory, a more or less complete picture of an individual's private life can be obtained through the linkage of the many databases, including those of the locationisers. The likelihood of such environment is only increasing especially in the law enforcement and national security domain since these are able to overrule privacy enhancing technologies.
Thus, for balancing privacy and national security for provider controlled data, technology provides very limited opportunities to protect the right to privacy. The balancing has then be left to a decision in the extent to which technological advances may be used for national security purposes.
For use controlled devices, including the control of the location data in active GPS devices, privacy may be enhanced through awareness building among (ignorant) users.

With respect to the impact of technology on the balance between location privacy and national security, cell-phone technology does not provide much privacy enhancement. Organisational difficulties to get to the data are the most likely barrier for security and intelligence services. Technological or legal barriers do not seem to exist at least if the required technology is available to the security and intelligence services.
Location technology does provide security and intelligence services with the means to track and trace individuals at varying levels of accuracy. Especially hybrid equipment, using both cell-phone technology and navigation technology allow for increased positioning of mobile equipment. In 2007, Nokia, world's leading mobile phone supplier and a leading supplier of mobile and fixed telecom networks, took over map maker Navteq for over US$ 8 billion. The new market of location based services requires accurate positioning of cell-phones which is accomplished with GPS featured cell-phones. These are now installed in top-of-the-line phones but are expected to be part of any phone in the very near future. This will result in a take-it-or-leave-it situation where consumers will not have a choice in the features coming with the cell-phone. The market of the privacy-aware might not be such that this development can be stopped or alternatives provided.
One scholar has argued that as a consequence of modern technology and loose privacy legislation "the terrorist will have no place to hide. But then, there's a chance that neither will we" (O'Harrow Jr. 2005, p.10).

7 The Netherlands: Balancing privacy and national security

This chapter focuses on the way privacy and national security interests are balanced with respect to the use of location information of mobile devices for national security purposes in the Netherlands. First, it addresses how privacy as a general concept is considered in the Netherlands. In the second section, Dutch national security is addressed and practical information on surveillance provided. In section 3, adherence to the six principles as provide din chapter 3 is assessed. Section four addresses the overall balancing of national security and privacy in the Netherlands five. Section six, finally provides the conclusion and improvements for balancing national security and privacy.

7.1 Privacy in the Netherlands

According to privacy international, the privacy situation in the Netherlands can be characterised as a systematic failure to uphold privacy safeguards (Rotenberg et al. 2006). Especially the categories privacy enforcement, data sharing, visual surveillance, communication interception and law enforcement access were categorised in the lowest categories of 'few safeguards, widespread practice of surveillance' and 'extensive surveillance/ leading in bad practice'.

In 2007, however, Verhue found that Dutch citizens have a great trust in the use of their personal data by government agencies. A majority of respondents considered the infringing means not unreasonable, and responded positive to the statement that the security of society increases when government knows more about their citizens. The high trust in government use of personal data makes that severe security measures are not considered as a major threat for the personal freedom (Verhue 2007, p. 3; translation BVL). Also the *Raad van Hoofcommissarissen* (Board of Superintendent Commissioners) (2004, p.41) recommends to increase policing mandates and found privacy regulations a barrier for further use of forensic investigations. Some politicians have found in these research results support for or justification for introducing means or mandates that push the balance between privacy and national security or law enforcement towards the latter (speech J.P. Balkenende at CvTIVD 2007 conference).

Citizens, however, may underestimate the impact privacy invasions may have for the way they live their lives. The Dutch Data Protection Agency (Kohnstamm et al. 2007) warns the naïve Dutch for the potential drawbacks of an 'omniscient' government. Stokmans (2007) adds that the average citizen is so naive because he does not know what personal data government may process and what the possible impact may be. Personal data registered at the Kadaster may be commonly known, as is the national license plate registration (with the *Rijksdienst voor het Wegverkeer*). But how many are, for example, aware of the *Justitieel Documentatie system*, a system registering natural and legal persons that have been, in one way or another, in contact with the Ministry of Justice (and affiliated agencies), including over 4 million natural persons (AIV 2007, p.41). "Thinking that what has happened to someone else will not happen to you is a mistake. Just as the idea that you do not have to fear government" (Stokmans 2007, citing professor Van Gunsteren, translation BVL). Tokmetzis (2007) shows what is currently possible and provides examples of mistakes of the data interpretation of law enforcement with a major impact on innocent citizens life. The *Adviescommissie Informatiestromen Veiligheid* (AIV 2007, p.8) concluded that the few academics and privacy advocates are right on in their fears for the increasing number of data requests of intelligence and law enforcement agencies and assessed these to be inappropriate. In addition, the commission points out that government insufficiently addresses the balancing of the fundamental

rights of privacy and security. The start of the www.ikhebnietsteverbergen.nl (I have nothing to hide website) can be explained as a way to make the ignorant Dutch citizen aware of what is already available to government and how this may influence one's autonomy and informational privacy.

It is argued that there is an invasion of the right to privacy if a more or less complete picture is obtained of certain aspects of the individual's private life (Kamerstukken 98-99, 25403, nr. 25, p.4). This does not include the observation that someone is driving a BMW or plays soccer (HR 21 March 2000 LJN AA5254). Buruma (2001, p. 34 - 35) found in Dutch case law that privacy should be considered as a way to be unrestrained oneself (referring to HR 19 March 1997, HR 9 January 1987, HR 19 February 1991). Also the term reasonable expectation has been used by the Supreme Court (HR 19 December 1995; HR 12 February 2002 LJN AD9222).
Privacy infringements in (semi-)public areas may not exist since people should be aware that in such areas that one can be observed, including audit observations, by others (HR 2 June 1998, HR NJ 1995, 684; Kamerstukken 1996-1997 25403, nr. 3, p.38). Later the Supreme Court was more nuanced stating that instances where a pattern of behaviour is made visible involves an aspect of the personal sphere that can be observed by everyone is a less far-reaching infringement than a pattern of behaviour where this concerns an aspect of the private sphere that deserves special protection such as a meeting or pattern of behaviour in a private house. In instances where observation results in visibility and reproducibility of the behaviour of the observed where he could reasonably expect to be invisible for the outside world/ public is a more than limited infringement of the right to privacy (HR 12 February 2002 LJN AD9222 at 60).
Observations of cell-phones or suitcases may interfere with the right to privacy since these items are so closely bound to the observation of individuals that they cannot be judged independently from these individuals (Kamerstukken 1996-97 25403 nr. 3 p. 28).

Adviescommissie Informatiestromen Veiligheid (Advisory Commission Information Flows in the Security Domain)

In February 2007, the Minister of the Interior, also on behalf of the Minsiters of Defence and Justice ordered an investigation of the system of information flows from (major) data files in the security domain available in both public and private sector. The security domain includes crisis management, and activities aimed at fighting crime and terrorism.
The Commission Information Flows in the Security Domain was created to perform the investigation. Their report (Data voor Daadkracht) concluded that the current system of information flows from external databases for security purposes does not meet the standards of proportionality, subsidiarity, and effectiveness. Furhter, it concluded that the balance between national security and privacy requires strategic attention to prevent a situation in which the balance between national security and privacy disappears.

7.2 National security in the Netherlands

National security has not been defined in law. However, a recent strategy document addresses the Dutch interpretation of national security (see Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2007).
National security is at stake if the vital interest of the state or society are threatened in a way that society (potentially) is disrupted (Minister of the Interior 2007, p.6 translation BVL). Vital interests of the state or society are (Minister of the Interior 2007, p.10 translation BVL): territorial security, economic security, ecological safety, physical safety (public health) and social and political stability (for example, respect for the core values of society such as freedom of speech and privacy). The operational value of this document is very limited since almost any action can be justified by using one of these broad terms.
Thus, national security concerns both security and safety aspects. Infringements by human acts are within the security category. Infringements by natural disasters, system or process errors, human failure or natural abnormal situations such as extreme weather conditions may be referred to as safety aspects (Minister of the Interior 2007, p.6 translation BVL).

The Dutch legislator explains the term national security as at least everything the tasks of the national security and intelligence service includes (see 25877 nummer 58a Eerste Kamer, 1; cf. o.a. Kamerstukken II 1999/2000, 25 877, nr. 8, p. 18; Kamerstukken II 2000/01, 25 877, nr. 14, p. 7).
Recent threats to Dutch national security include the murder of Theo van Gogh, and very recently the activities of Animal activists (*Dieren Bevrijdings Front*) making a constructor stop his constructions work for a life science business park (see Staal 2008) .

Protecting national security in the Netherlands

The Dutch Intelligence and Security Service *(Algemene Inlichtingen- en Veiligheidsdienst*, further AIVD) is the Dutch civilian intelligence agency. It 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 (article 6 WIV 2002). Current areas of interest of the AIVD are terrorism, radical developments, salafism, left and rightwing extremism, undesired involvement by foreign powers, proliferation of weapons of mass destruction, foreign intelligences, and stimulating security (website AIVD). These are, however, general categories that are subject to change. Main focus of the AIVD is currently religious extremism and terrorism (Van Hulst 2007). The Service employs approximately 1500 people (Van Hulst 2007). [16]

7.2.1 Role of location information in protecting national security

AIVD Director Akerboom stated that contra-terrorism aims at stopping the terrorist or a terrorist group to reduce the terrorist threat (Akerboom 2003). Detecting potential terrorists includes revealing their networks. This implies that data concerning the type of person, their role in the network, their contacts, their ideological background, and other countries involved needs to be included in the analyses (see Akerboom 2003). Modern technologies may be used to obtain insight in the threatening networks, e.g., to identify travel behaviour of potential terrorists (Akerboom 2003). The use of identification data or traffic data may in many instances provide sufficient information to satisfy these needs. Concerning location data, ex-post location data, including location data from the stand-by mode of a mobile device, is

[16] The Military Intelligence and Security Service (*Militaire Inlichtingen- en Veiligheidsdienst*, MIVD) is the military counterpart of the AIVD. The MIVD protects the interests of the Netherlands in instances where the armed forces may be involved. For detailed information we refer to the WIV 2002 article 7). It has approximately 700 employees (website MIVD).

likely to address the needs of the AIVD in many instances for the purpose of revealing a terrorist network. Real-time location data processing might be useful in combination with or to complement observation means. Real-time location data processing by itself would be beneficial if this could contribute to the prevention of an event threatening the national security.

The AIVD has three primary sources of information:

- open sources such as the internet, libraries, among others;
- delivered information by citizens, companies, other government agencies, and foreign security and intelligence services, and
- acquired information; information for which a special means mandate is required.

Identification, traffic and location data of mobile devices are within the acquired information category.

7.2.2 Practice of surveillance

On tracking and tracing of cell-phones no current public quantitative information is available. Telecom providers are prohibited to publish data concerning number of phone taps (*Besluit beveiliging gegevens aftappen telecommunicatie*, art. 6). Concerning phone taps only relatively old information has become public. This may give some insight in the use of special means mandates for law enforcement.
The number of tap orders for law enforcement was in 1998 approximately 10,000. Three thousands were on traditional phones, and 7,000 on mobile phones (Kamerstukken 2000-2001 27591 nr. 2, under nr. 68; see also Kamerstukken 2002-2003 aanhangsel van de handelingen 1035). The minister did not see any added value in centrally registering the number of phone taps. He did not have any evidence that the number of suspects being tapped had significantly increased. However, the number of taps increased because suspects have now more communication means at their disposal, which results in more taps.
One research claims that other countries have fewer phone taps per citizen (see Albrecht et al. 2003). The Dutch Minister has explained that this may be due to the use of other means, which are in the Netherlands considered as infringing the privacy more than phone taps, such as infiltration, storing confidential information and house searches (Kamerstukken 2002-2003 aanhangsel van de handelingen 1035).
AIV (2007, p.48) did only find data on the number of requests for data concerning subscribers or 'owners' of telecommunication means in the *Centraal Informatiepunt Onderzoek Telecommunicatie* (Central Information Point Research Telecommunication, CIOT). This centre updates on a daily basis the identification data of the owners of telecommunication means, provided by the telecom operators. The number of requests increased from 722,000 in 2003 to 1,220,000 in 2005 and over 1,800,000 in 2006. Police requested 93% of these, special law enforcement agencies (*bijzondere opsporingsdiensten*) 3% and AIVD 4% (AIV 2007, p.48).
For the Dutch security and intelligence services no figures are available. The AIVD refuses to report these data because of reasons of national security. The Advisory Commission on Information Flows in Security finds this not very convincing since it concerns only information on total number of phone taps and the extent to which these develop (AIV 2007, p.95). The Minister of the Interior provides and discusses the number of taps and their nature with the parliamentary Commission for the Intelligence and Security Services (Kamerstukken 2002-2003 aanhangsel van de handelingen 1553 under 1). Further, the Review Commission assesses the nature of the taps (Kamerstukken 2002-2003 aanhangsel van de handelingen 1553 under 1).

Provided the 10,000 phone taps from 1998 and the relative increase in phone taps in Germany over the period 1998-2006, one may argue that the current number of phone taps in the Netherlands for law enforcement is in the range of 3,000 for traditional phones and 40,000 for cell-phones. Based on the AIV percentages for the cell-phone identification data, this 40,000 might be 93% of the total cell-phone taps. If AIVD accounts for 4% of the total, the number of cellphone taps by AIVD might total 1,700 phone taps per year. Van de Pol (2006, p. 41) has assessed the total number of taps in the range of 30,000 to 50,000.
On 27 May 2008, the Minister revealed that for the second part of 2007 for 12,491 phone numbers tap orders were provided to law enforcement (Minister of Justice 2008). These concerned 10,490 (84%) cellphone numbers. On average, every day almost 1,700 taps are processed. Although it is not specified what the second part of 2007 exactly is, the total number of new tap orders for 2007 may be in the range of 25,000 phone numbers. No data was provided on the amount of phone numbers for which traffic data or location data was requested. Nor data on the use of taps or telecommunication data by the AVID were provided. Also information on the number of internet taps is scant. One exception are the numbers of the Dutch national association for internet providers (NBIP), representing 44 providers together serving 1.5 million customers. They stated that 31 users were tapped in 2006, coming from 23 in 2004 and 40 in 2005. The average length of a tap was around 2 months (Ringelestijn 2006).

7.3 Balancing national security needs with privacy

In chapter 3, six principles were provided to which personal data processing should adhere if it was to respect international law. These principles are:

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.

Principle 5: guaranteed accuracy of the data for the purposes of use.

Principle 6: individual participation in the process whenever possible.

In this section, we will provide for each principle an assessment of the extent to which the Netherlands adheres to these principles.

7.3.1 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 Netherlands, the invasion of a constitutional right requires a decision based on a formal law (CBP 2004, p.32). Thus, the wide interpretation of the ECtHR of the 'some basis in domestic law' (including administrative rulings or procedures) does not apply to the Netherlands.

The right to privacy finds its basis in the constitution in article 10. This article reads:

1. Everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by or pursuant to Act of parliament.
2. Rules to protect privacy shall be laid down by Act of parliament in connection with the recording and dissemination of personal data.
3. Rules concerning the rights of persons to be informed of data recorded concerning them and of the use that is made thereof, and to have such data corrected shall be laid down by Act of parliament. (translation by IVIR, 2005)

The Dutch constitution is the fundamental legal basis in the protection of privacy in the Netherlands. In addition, European legislation provides an additional basis for Dutch legislation. The data protection act (*Wet bescherming persoonsgegevens*, Wbp) implements Directive 46/95/EC into Dutch legislation. It provides the legal framework for the processing of personal data. Personal data may, for example, only be processed for specified and legitimate purposes (art. 7), and purposes not conflicting with the initial purposes for which they were acquired (art. 9), and no longer stored than strictly necessary (art. 10). The implementation of Directive 2002/58/EC in the Telecommunication Act (Tw) interlinks with the WIV 2002.
However, Directive 95/46/EC and Directive 2002/58/EC do not necessarily apply to processing of personal data concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law. Member States have the freedom to restrict certain provisions of these Directives. Accordingly, the Wbp and the Telecommunication Act do not apply to the processing of personal data for purposes of national security (Wbp art. 2b, art. 43a; Explanatory Memorandum WIV 2002, p. 66).
Interference for purposes of national security finds its basis in the *Wet op de inlichtingen- en veiligheidsdiensten 2002* (WIV 2002, Act on the Intelligence and Security Services 2002), a special law that allows for the existence of the intelligence services, and details the tasks and means at the disposal of the two services (civilian and military). The law arranges for the situations in which the intelligence services may be involved and the means they may use to protect national security.
Other relevant legislation are the Decree ex article 28 WIV 2002 and the Decree appointing topics ex. articles 6 and 7 WIV 2002. Further, the implementation Act of the Data Retention Directive 2006/24/EU has been introduced in parliament (*Wetsvoorstel bewaarplicht telecommunicatiegegevens* (Kamerstukken 2006-2007 nr. 31145)).

Transparency in what data can be claimed

Starting point of the implementation of Directive 2002/58/EC in the Telecommunication act is that the processing of data is only allowed if and as long as this is necessary for the provision of the telecommunication service, including the billing process (art. 11.5a (3) Tw). Location data only can be processed if they are anonymous, or non-anonymous if the user has given his consent (art. 11.5a Tw).

However, the providers must now provide the requested data to intelligence services and law enforcement agencies as these are authorized to request telecom providers to provide data on a specific user and his telecommunication traffic (art. 28. 1 WIV 2002; see also Tw art. 13.2, 13.2a, 13.2b, and art. 13.4j). The data request, however, can only concern: the name, address of the user; numbers of the user; name, address and the number of the receiver; the day and time of the connection; the location data of the equipment in case of a connection or an attempt to connect; the kind of services used; the name and address of the person paying the phone bill (art. 2 Decree ex article 28 WIV 2002).
Concerning the location data of the equipment, the AIVD is only allowed to request the data that are directly related to the use of the equipment. Location data can only be used for tracking if the user communicates 'actively' (e.g., using the phone to call or to SMS). It is explicitly prohibited to claim data from providers that would allow the AIVD to trace a person on a continuous basis through the stand-by mode of his cell-phone (Explanatory Memorandum to the Decree ex article 28 WIV 2002). Further, the telecom provider must cooperate with the national security and intelligence service to decipher encrypted conversation, telecommunication, and data (WIV 2002 art. 25, Tw art. 13). Another relevant article is article 13.1 Tw: Providers of public telecommunication networks and public telecommunication services only make their networks and services available to users if these networks and services are tappable.

Transparency of the means available to intelligence agency
The WIV 2002 specifies exhaustive (*uitputtend*) the means that may be used, the authority required to consent and prescribes a maximum time to the use of these means. When what means may be used is described in rather vague terms. Legitimate reasons for the processing of personal data are: a severe suspicion that the objectives of a person or organisation may result in a danger for the continuing existence of the democracy, or the security or other major interests of the state (art. 13.1 a WIV 2002). Also the requirements are rather vague and subject to change overtime. In the past, members of the communist party would have been, and were, subject to surveillance. Now members of Islamic organisations are more likely to be traced than a member of GroenLinks (left-oriented political party).

In conclusion, the Wbp and Tw provide the framework for the data processing for all purposes except for purposes of national security and preventing, tracing and prosecuting criminal acts. For the former the WIV 2002 and the Decree ex article 28 WIV 2002 provide the framework for the balance between privacy and national security. For the latter it is the Code on Criminal Proceedings, the Act on the police registers and Act on special authorities for law enforcement.
With the implementation of the WIV 2002, the Dutch' legislative framework meets the requirements of principle 1 for the activities of the national security and intelligence service.

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

In the Netherlands, the test of legitimacy is being used for striking a fair balance between de demands of the general interest and the interest of the individual. The test includes four criteria (Commissie van Toezicht, jaarverslag 2004-2005):

- The necessity criterion (art. 12.2, 14.1, 18 WIV 2002);
- The subsidiary criterion (art. 31 lid 2 WIV 2002);
- The proportionality criterion (art. 31 lid 3 and 4), and the
- Duty of care (art. 15 and 16 WIV 2002)).

The Dutch Supreme Court has followed the ECtHR judgments in its rulings of *Van Baggum* and *Valkenier* that interference with the right to privacy should be in accordance with the law and necessary in a democratic society to protect specific interests (see also Kamerstukken 22036 nr. 6).

The necessity criterion

The AIVD can process personal data only if this is necessary for the execution of the WIV 2002 (art. 12.2) or the Act security investigations (*Wet Veiligheidsonderzoeken*).

When the Minister of the Interior has decided that one of the core interests of the state is in danger, it must be determined whether the national security and intelligence service needs to be involved. The necessity of the involvement of the national security and intelligence service is based on a risk analysis accomplished by the security and intelligence service. The analysis focuses on the nature, seriousness and the impact of the risks. It assesses also the relation between a (national) interest, the threat to this (potential) interest and the resistance of the responsible agency (belangendrager). This assessment results in the safety risk. The result of the assessment may be that the national security and intelligence service is activated (Commissie bestuurlijke evaluatie AIVD 2004, p.57).

The assessment is primarily based on the experiences and prediction ability of the AIVD. The Commissie bestuurlijke evaluatie AIVD (2004, p.60) concluded that it is not completely clear what the direct reason may be to start a risk assessment and to decide for a team assignment. After a bureaucratic procedure (see Figure 7-1) an investigation may start.

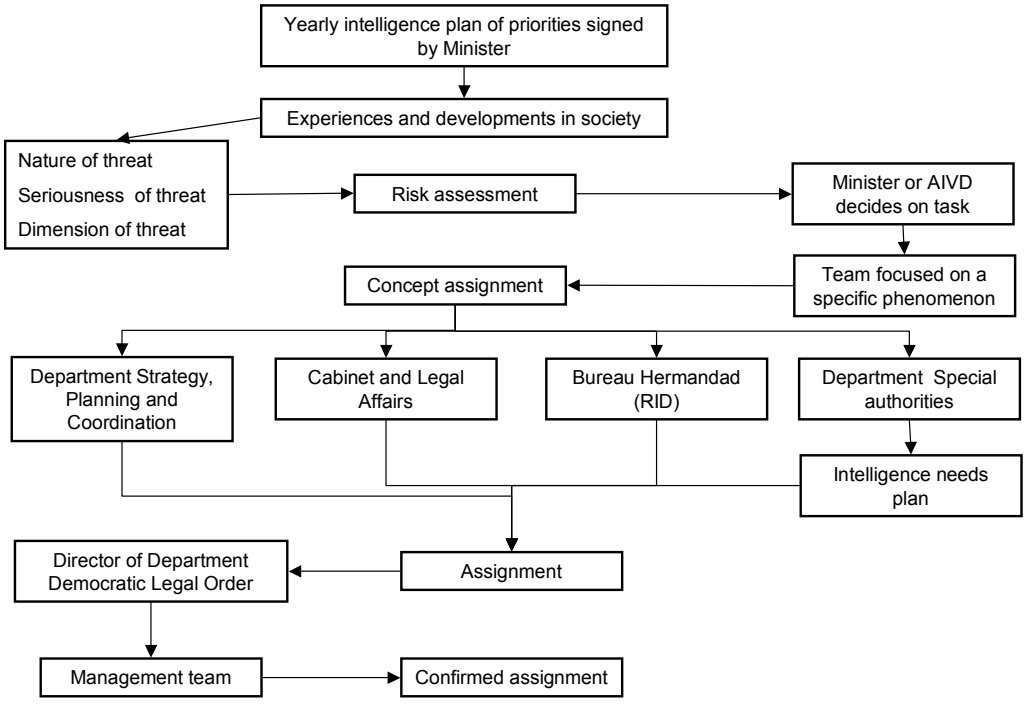


Figure 7-1 Decision making process in the formulation of an assignment (Source: Commissie bestuurlijke evaluatie AIVD 2004, p.124, 58-60)

If the Minister of the Interior decides that the national security and intelligence service will be involved, the question is how? First, a threat analysis should clarify which part of the threat needs to be addressed by the national security and intelligence service. Further, the intelligence service assesses the time pressure to neutralize the threat and which data are already available and which are lacking. Based on the threat analysis, the Minister or the head of the intelligence service decides which (special) means is going to be utilized to acquire the needed (and lacking) information. The lacking information can be acquired through public sources (newspapers, internet, and other public data sources) or information sources, which are available to the national security and intelligence service (people register, police register). If this is impossible or not possible in the available time frame, or the acquired information is with reasonable doubt assessed to be incomplete or inaccurate, the national security and intelligence service may utilize its special authorities (Explanatory Memorandum WIV 2002, p. 52). The use of special authorities is bound to the criteria of subsidiary and proportionality.

Commissie bestuurlijke evaluatie Algemene Inlichtingen- en Veiligheidsdienst (Commission Administrative Evaluation Dutch Intelligence and Security Services; Commission Havermans)

9/11 and several other events (assassination Fortuyn, decision of parliament to participate in the war in Iraq) has resulted in increased attention to the functioning of the Intelligence and Security Services in the Netherlands. In 2003, after the parliamentary discussion on the marriage of Prince Johan Friso and Miss Wisse Smit, the Minister of the Interior introduced and commenced the 'Commission Administrative Evaluation Dutch Intelligence and Security Services' to perform an administrative evaluation of the legal tasks, responsibilities, authorities, and means available to the AIVD and the way the AIVD anticipates on these, provided the changes in society. Three questions were leading in this research:

1. Which expectations does the political-administrative environment have about the task of the AIVD, provided the changes within society?
2. How does the AIVD execute its tasks and responsibilities and how can these be improved?
3. Are the authorities and available means (both quantitative and qualitative) to the AVID sufficient to meet the requirements and expectations?

The Commission published its research in 2004.

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

The WIV 2002 provides the decision framework with respect to proportionality and subsidiarity concerning each of the special authorities for specific cases. This general framework is further developed in internal procedures. These provide for each special means how to decide to use them. It addresses the procedure, the objective, the instances when a special means can be used, required permissions, the request to use it, the test, the decision, notification, relevant legislation and how it should be used. Concerning proportionality and subsidiarity, advise is provided by a department focusing on the use of special authorities (*directie Bi-*

jzondere Inlichtingenmiddelen) (Commissie bestuurlijke evaluatie AIVD 2004, p. 126). Figure 7.1 provides an overview of the decision making process within the AIVD, ultimately resulting in an approved task assignment. In 2004, the Commission bestuurlijke evaluatie AIVD confirmed that the AIVD is strictly working according to these procedures concerning the use of special authorities (see Commissie bestuurlijke evaluatie AIVD 2004, p. 126).

Criterion of subsidiary

The ECtHR has ruled that the purpose for which the personal data are processed can in all fairness not be realised in another manner, which has a less negative impact for the person concerned (Wbp 25892 nr. 3; see also Commissie van Toezicht, jaarverslag 2004-2005, 32-33). The subsidiary criterion rules that if it is decided that the processing of (personal) data is needed through a means falling under the special means regime, then the national security and intelligence service is required to select adequate means that are the least harmful for the person or party concerned (art. 31.2 WIV 2002). Use of special authorities is not allowed if they unreasonably disadvantage the individual concerned (art. 31 WIV).

The use of special authorities is only allowed if the data cannot or not in time be gathered through public sources or information sources to which the security and intelligence service has been granted a right of access (*kennisneming*) (art. 31 WIV).

Criterion of proportionality

In addition to the requirement of subsidiary, the use of special means also need to be proportionate to the legitimate aim pursued (art. 31.4 WIV 2002; Explanatory Memorandum WIV 2002, p.53). The Explanatory Memorandum provides the following example: If the aim can be reached to obtain data concerning people visiting a specific house through a camera outside the house, then the use of a camera inside the house is disproportionate to the aim pursued. This is the norm as provided in the law. The Explanatory Memorandum clarifies that the norm is so general since it needs to be useful in a wide variety of situations (Explanatory Memorandum WIV 2002, p. 51).

The Minister of the Interior has assessed that it is impossible to rank the special authorities. He argued that the execution of one special power is not necessarily more or less infringing one's right to privacy than others. For example, is observing and following someone for four weeks more infringing than a phone tap for four weeks? (Explanatory Memorandum WIV 2002, p. 41). Is video observation (static observation) a greater interference in the private life than tracing a person (dynamic observation)? (Explanatory Memorandum WIV 2002, p. 51).

The Dutch data protection agency (*College bescherming persoonsgegevens*) holds as a rule of thumb that a citizen's expectation of privacy in public areas is generally less than in his house or at work (CBP 2004, p.9). Privacy infringing surveillance may include the observation of individuals in places they have a high expectation of privacy (CBP 2004, p.23). Also in chapter 3 we cited several researches and ECtHR rulings that indicate that video surveillance in public areas is considered less infringing than real-time tracking.

The Explanatory Memorandum of the WIV 2002 further adds an additional requirement to the principles of the European Court: the most effective and efficient means available should be used (Explanatory Memorandum WIV 2002, p. 52). An average phone tap has been assessed to cost €9,450 (without administrative and other cost, see AIV 2007, p.49 referring to press release of NBIP).

Duty of care

The WIV 2002 rules that the use of a special means is immediately stopped if the aim pursued has been reached or if the aim can be reached with less intruding means (art.. 32).

The *Adviescommissie Informatiestromen Veiligheid* (AIV 2007, p.58), however, did not find a clear decision framework (toetsingskader) to which data requests of AIVD or law enforcement should adhere, for example on the process of requesting data.

According to both public and private data providers often the request for information is non-specific, lacking a (sound) formal basis, and concerns an unreasonably large amount of data. In addition, the research found that 'more than once' identical requests were made by different agencies (AIV 2007, pp. 65, 102). Together, this made the Commission conclude that the data acquisition process of the intelligence and law enforcement is ineffective. Each agency uses a different approach, and there is uncontrolled increase of the number of data requests (interviewees in this research were unable to explain this development).

Because the data requesters do not or only pay marginally for the data, they are not confronted with the true financial consequences of their requests. Therefore no incentive exists to cope effectively or efficiently with the data requests (AIV 2007, p. 100).

Available means and required permissions

The decision making process concerning the national security and intelligence service takes place in the periodic meeting of the responsible Ministers (i.e. of the interior, defence, and the prime-minister, and if necessary other Ministers). Dutch law distinguishes between the infringement of the means and the authority required to consent.

Not all types of special means require the same permission, thus at least suggesting an order of infringement. The greater the infringement the higher the authority that needs to consent. Table 7-1 shows the means available under the special means provision of the WIV 2002 Act. For the opening of a letter the Court in The Hague needs to consent. The next most sensitive category is related to intrusions to one's home, such as searching homes or installing observation equipment in homes. Also wiretapping is within this category. The following category includes the physical surveillance, and undercover activities. The least sensitive category includes (location) data of telecom providers, amongst others. The Minister assessed that the processing of traffic data is less infringing than a phone tap where private conversations can be heard (Explanatory Memorandum WIV 2002, p. 47). Therefore, for a traffic data request a lower authority is required than for a phone tap.

Activity	Period of activity	Permission of
Opening paper letters	Max. of three months per request	Court in The Hague (art. 23)
Installing observation means in homes	Max. of three months per request	Minister of the Interior in writing (art. 20.3)
Searching homes	Max. of three days	Minister of the Interior in writing
Wiring, receiving, recording, eavesdropping including deciphering encryption (of conversations, telecommunication or data transmission through an automated work)	Max. of three months per request	Minister of the Interior (art. 25)
Recording non cable telecommunication (personal data)	Max. of three months per request	Minister of the Interior (art. 26. 4)
Searching places and objects	Max. of three days	Minister of the Interior or on his behalf the head of the AIVD (art. 22.1 a)
Undercover activities	Not specified	Minister of the Interior or on his behalf the head of the AIVD (art. 21)
Observing people	Max. of three months per request	Minister of the Interior or on his behalf the head of the AIVD (art. 20.1 a)
Tracking people	Max. of three months per request	Minister of the Interior or on his behalf the head of the AIVD (art. 20.1. b)
Installing observation means (no homes)		Head of the AIVD (art. 30.1)

Table 7-1 Availability of means for AIVD and required permission

Also within the 'data category' different regimes exist (see Table 7-2). Sensitive data, before categorised as special personal data category, can only be processed if this is inevitable. Other sensitive information, information concerning labour union membership or membership of a political party, can be requested by an AIVD officer, however. The Minister thinks this deviating policy is justified because someone's political preferences might be crucial in the assessment of the potential danger for national security (Explanatory Memorandum WIV 2002). Similarly, it is inevitable to process sensitive personal data concerning religious or philosophical beliefs if these are used to justify anti-democratic, dangerous to the State, or anti-military activities, or in the instance of terrorist activities of religious (splinter) groups (Explanatory Memorandum WIV 2002).
Further, for the processing of the content of email or conversations consent of Minister of the Interior is needed. The Head of the AIVD can request other processed data, including (real-time) location data of the mobile device. Identifying information, such as name and address, can be required on behalf of the Head of the AIVD. However, the AIVD cannot require telecom providers to provide data concerning location of a mobile device in the stand-by mode. Such data may be acquired through the placement of a 'beeping device' on the cellphone (art. 20 WIV 2002), or through a communication tap (Art. 25 WIV 2002).

Type of data (WIV 2002)	Examples	Decision/ Requisition by	WIV 2002 article
User data	Name, address, number and type of service used	Head of the AIVD or on his behalf	Art. 29
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 the AIVD	Art. 28(1);; Besluit ex artikel 28 WIV 2002, art. 2, Besluit ex art. 28 WIV (art. 2(f))
Traffic data	Historical and future location data of cell-phone if actively been used, date and time of use	Head of the AIVD	Art. 28(1); Besluit ex artikel 28 WIV 2002, art. 2
Content of communications	Content of an email or voice mail[17]	Minister of the Interior	Art. 25
Certain stored data (3): other data	(Historical and future) location data of cell-phone in stand-by mode processed by telecommunication provider	Not allowed	Besluit ex artikel 28 WIV 2002
Data processed after requisition date and directly available to national security and intelligence	Real-time location data of cell-phone if actively been used	Head of the AIVD	Art. 28(1&4)
Sensitive data (1)	Data concerning racial or ethnic origin, religious or philosophical beliefs, or concerning health or sex life	Only allowed if inevitable	Art. 13(3)
Sensitive data (2)	Data concerning political opinions, trade-union membership	AIVD employee	Art. 17(1)
Other data	Data on savings, earnings, education, job (history), club membership, etc.	AIVD employee	Art. 17(1)

Table 7-2 Sensitiveness of data according to WIV 2002

For how long can location information of mobile devices be tracked and traced?

Table 7-1 shows the differences in the duration of the mandate for different data categories. Searches of objects and homes can last for maximum three days. The other special authorities have the standard maximum of three months. However, for telecommunication data no

[17] EK 2004-2005 29441 E, p.4; see Stcrt 16/10/2006, nr. 201 p. 14

maximum period is specified. The only requirement is that these data cannot be processed any longer than necessary.
The proposed Dutch implementation of the Data Retention Directive requires telecom providers to store telecom data for at least 18 months (Kamerstukken 2006-2007 nr. 31145)[18].

The categorisation of required consent for different activities may imply an order of privacy infringements. With respect to data, the following order was found in the WIV 2002 (from the most sensitive down):

- location data of cell-phone in stand-by mode
- Information concerning racial or ethnic origin, religious or philosophical beliefs, or concerning health or sex life
- Content of an email or voice mail
- Real-time location data of cell-phone if actively used
- Historical location data of cell-phone if actively been used (incl. date and time of use)
- Name, address, phone number, kind of service used
- Data concerning political opinions, trade-union membership

Further, from the subsidiary principle follows that if an interest of the AIVD can be satisfied through identifying information, there is no need to claim traffic data or location data. Similarly, if traffic data can satisfy the requirements, there is no need to process the more detailed location data. If historical location data can satisfy the needs than real-time location data should not be requested.

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

In the Netherlands, it depends on the intrusiveness of the means that are utilized who balances the general interest with the interest of the individual (see 7.3.3). For most means, the responsible Minister, or the head of the intelligence service has to decide on the interference. Only in the instance of interfering with the analogue letter secrecy a judge needs to consent. For (e-) surveillance the Dutch Minister of Interior needs to consent. There is no independent supervision over this decision.

Effective remedies

Internal use authorization
The AIVD takes care of the technical and organisational security measures to prevent unauthorised use and loss or damage to the data (art. 16 WIV 2002). Further, personal data will only be disseminated to an AIVD officer if this is necessary for the proper execution of the tasks attributed to him. Moreover, it is intended to keep the number of people that may access certain data as small as possible (Explanatory Memorandum WIV 2002, p.54).

Control mechanisms
The Review Commission (*Commissie van Toezicht*) is one of the independent controlling mechanisms outside the authority of the national security and intelligence service or Minister themselves. It has jurisdiction over the activities of the AIVD, the MIVD and other bodies to the extent that these carry out AIVD and MIVD activities. Also the coordinator of the in-

[18] On May 22, 2008, the coalition in parliament agreed on a 12 month retention period.

telligence services is subject to review of the Commission. The Commission assesses the legitimacy of the acts of the AIVD and advises the Minister on security issues (art. 64 WIV 2002). The Commission does not assess the effectiveness of the operations of the AIVD (Commissie van Toezicht 2004-2005).
A Royal Decree sets up the Commission, which consists of three members (art. 65 WIV 2002). The Minister selects each member from three candidates proposed by the parliament. The Commission should be provided all information that it thinks are necessary for the adequate execution of its' tasks (art. 73.1 WIV 2002). The Commission reports on its findings (art. 79.1 WIV 2002). Its capacity, 3 members and 4 supporting staff members (website CTIVD), limits its possibilities to review the AIVD (see Commissie bestuurlijke evaluatie AIVD 2004, p.91). In addition, the Commission cannot render any legally binding decision.

Review Committee on the Intelligence and Security Services

The Review Committee's task is to assess the legitimacy of the actions of the Dutch intelligence and security services. This supervision involves the civil intelligence and security service (the AIVD) and the military intelligence and security service (MIVD), as well as (parts of) a number of organisations in so far as these are active in the area of intelligence. The Review Committee can provide relevant ministers solicited and unsolicited information and advice on the Committee's findings. The Review Committee conducts in-depth investigations as well as random samples on the intelligence and security services.
The Committee also supervises the legitimacy of the implementation of the Security Screening Act (WVO), which provides rules for the security screening carried out by the services before a person may hold a so-called position involving confidentiality.

The Committee consist of:
- Ms I.P. Michiels van Kessenich-Hoogendam, chairman of the Committee
- A.H. van Delden, member of the Committee
- B.A. Lutken, member of the Committee

Further, parliament has enacted a Commission for the Intelligence and Security Services (Commissie voor de Inlichtingen- en Veiligheidsdiensten) with political leaders of most political parties (the Socialist Party, however, refused to participate). This commission discusses in strict secrecy the operational activities of the security and intelligence services.
Finally, article 78(2) WIV 2002 enables parliament to establish an expert body to report on a given matter. This power was used in 2004 to introduce the Commission Havermans.
The AIVD also sends a yearly report of the service to the national parliament (WIV 2002 art. 8.1). In the report it provides the current and former focus areas of the service. The Algemene Rekenkamer checks the financial situation of the AIVD.

Complaints
Anyone can file a complaint about the AIVD with the Minister of the Interior (for AIVD) or Defence (for MIVD). The AIVD is required to seek the advise of the Review Commission. The Minister provides his point of view after the consultation of the Review Commission. If the Minister's point of view does not satisfy the 'plaintiff', the complaint may be filed with the National Ombudsman. The Ombudsman can access secret files of the AIVD, on the condition that the content of the files remains secret. He judges the complaint and his state-

ment may be accompanied with recommendations for the national security and intelligence service. The Ombudsman cannot render legally binding decisions. It is unclear whether the AIVD should take these recommendations into account. The Ombudsman has reported in three instances on complaints about the AIVD (see Commissie bestuurlijke evaluatie AIVD 2004, p.92).

It has been suggested that citizens may file a suit under civil law. The civil judge, however, does not have and cannot require full access to the information of the security and intelligence services. It may therefore judge on the basis of insufficient information. Recently, the Review Commission responded to a civil court's ruling, which it found unjust based on secret information inaccessible to the judge (see Commissie van Toezicht 2006).

It has been suggested that the (critical) recommendations in the Review Commission's yearly report should be noticed by members of parliament which can question the Minister about it. With non-satisfying responses from the Minister, parliament may force the Minister to act upon/ implement the recommendations of the Review Commission. This is, however, a rather complex and uncertain process, which is not quite of the same order as a legally binding decision of an independent authority as the European Court recommends. One may also question whether this can be considered 'a true legal means against possible infringements' (*daadwerkelijk rechtsmiddel*) as the Dutch legislator has interpreted the effective remedy requirement of the ECtHR (see Kamerstukken 25877 nr. 58a EK, 10).

The Minister has argued that in the WIV 2002 an explicit choice has been made for a system in which the Minister is (politically) responsible for the activities/ performance of the AIVD. The Minister justifies its decisions ex-post to parliament, judges and the Review Commission of the AIVD. In such system, the Minister argues, a requirement of ex-ante permission through a court order does not fit well in a system of full ministerial responsibility (Kamerstukken 1997-1998, nr. 25877 nr 3, p.37). The same applies in the instance of involving an independent commission in the decision-making process for using a special means. A legally binding decision of such independent commission would limit the accountability of the Minister, and parliament could not call the commission to account (Kamerstukken 2005-2006, 29876 nr. 18).

Effective remedies imply that the conclusions of the independent review commission are respected by the AIVD and the recommendations used to improve the performance of the AIVD. Overall, this system aimed at improving the overall performance of the AIVD is effective in the Netherlands. However, for individuals with complaints on the AIVD this voluntary system is inadequate. The ECtHR is the only institute that will provide a fully informed legally binding decision on the activity of the AIVD. Civil Dutch Courts may not decide fully informed, and those institutes that may be fully informed cannot render a legally binding decision. Therefore, we conclude that it is unlikely that the present Dutch remedy would pass as effective when a case would be brought before the ECtHR (cf. Cameron 2007, p. 57; Loof 2006, p. 833; ROB 2005, p. 46, see also Supreme Court in *Van Baggum*).

The Advisory Commission on Information Flows in Security (2007) noticed that a kind of independent review with specific focus on the use of external databases by intelligence and law enforcement agencies can positively contribute to the process (of data acquisition and use) involved, and to the duty of care and the way privacy is protected. Others (Kuitenbouwer 2007) suggested to introduce an inspector-general for the AIVD.

7.3.5 Principle 5: guaranteed accuracy of the data for the purposes of use.

The WIV 2002 requires that the data processing is careful and adequate (art. 12.3; art. 6(a)). Metadata accompanies the data to indicate the reliability of the data or the source of the data (Art. 12.4 WIV 2002). Further, the AIVD should take care of adequate facilities to ensure that the data processed are correct and complete.

In 2004, the risk-assessment was primarily based on open sources and considered to be problematic (Commissie bestuurlijke evaluatie AIVD 2004, p.189). The reliability of the AIVD assessment of the seriousness and likelihood of an event was often questioned by law enforcement agencies (Commissie bestuurlijke evaluatie AIVD 2004, p.185).

The *Adviescommissie Informatiestromen Veiligheid* (AIV 2007, p.25) noted that of all aspects of intelligence, the collection of data and its quality is barely paid attention to by politicians and administrators. In addition, Neve et al. (2006, §4.3.4) refer to the US where means to acquire and process data resulted in an overload of data often of poor quality making it difficult to find patterns from the data. The Commission bestuurlijke evaluatie AIVD (2004, p.63) noted that also for the AIVD the amount of data to be processed has increased significantly, but the 'informatisation' of the AIVD has not developed at the same pace.

It is unclear whether the AIVD obeys the rules for data requests and processing (AIV 2007, p.11).

Transparency of the human sources used is not required by law. This relates to the need to keep human sources of the AIVD confidential, in order to protect the source (Explanatory Memorandum WIV 2002, p.66). This makes it difficult to assess the extent of adherence to this principle.

The AIV (2007) concluded that the security of data (processing) should be improved to meet required standards.

7.3.6 Principle 6: individual participation in the process whenever possible.

Individual participation in secret personal data processing is difficult to establish. In the Netherlands, people can request information about which personal data, if any, is being or has been processed by the national security and intelligence service (art. 47.1 WIV 2002). A person whose personal data is or has been processed by the national security and intelligence service can ask the national security and intelligence service to correct, add, or delete information (Art. 43. 1). The responsible Minister decides that requests for information on processed personal data are denied if data concerning the requestor are being or have been processed, unless:

- the data concerned was processed more than five years ago;
- there are no new data added;
- the personal data are irrelevant for current investigations (art. 53.1 a WIV 2002).

Access is also denied if no personal data has been or is processed (art. 53.1 b WIV 2002). Appeal to the Court in The Hague is available (art. 57 WIV 2002).

7.4 Developments in law in the Netherlands

"De opsporingshond is van nature aangelijnd, in tegenstelling tot de losgebroken misdaadhond, maar hij valt nauwelijks te houden, zozeer trekt de misdaadhond hem aan, en in zijn kielzog trekt hij de wetgevende wachtpost met zich mee."
(Koops 2006, p. 46)

In the Netherlands, the margin of appreciation has increasingly been stretched towards national security interests (see Koops 2006, p. 18-19). For example, since 1 July 2005, providers of telecommunication networks and services are required to provide on request the intelligence services with data concerning a user and the telecommunication traffic with regard to this user. They are, however, still within the European legal boundaries.

Although the Commission bestuurlijke evaluatie AIVD (2004, p.124) and also the Intelligence and Security Agency itself (see letter of the Minister of Interior affairs to the Tweede Kamer, 19 juni 2004) found the available means to protect national security sufficient, the available means have since then been extended.
In May 2006, a new Article 29a WIV2002 was proposed. It requires authorities responsible for financial services (banks, credit card organisations, credit organisations) or those operating as a provider of traffic services (airport, airlines, ferries, public transportation, etc.) to provide data to the intelligence services (Kamerstukken 30553; introduced 18 May 2006). It broadens telecommunication providers to all communication providers, delegates the exact data to be requested to a Ministerial Decree, and will ignore data collection and use principles in allowing data analyses on anyone. This bill is still under discussion. Such requirements may not be necessary since most providers provide the requested data (see Explanatory Memorandum 30553 nr. 3; Kamerstukken 30553 nr. 4 (Advies Raad van State en Nader Rapport); CBP 2007b)[19].
The Data Retention Directive requires to store telecommunication data for a minimum of six months . For its implementation into Dutch national legislation, the Minister has proposed a term of 18 months without justifying it with supportive evidence on the positive effect compared to the minimum term.
Concerning the location data of terminal equipment, the Dutch intelligence services are currently only allowed to request data that are directly related to the use of the equipment'. It is explicitly prohibited to trace a person on a continuous basis through the stand-by mode of his cell-phone (Nota van toelichting Besluit ex artikel 28 WIV 2002, Stb. 289 (2005) art. 2e).
However, in line with the recent developments, it is conceivable that in the near future a situation will emerge where the national security and intelligence services will be allowed to track a person continuously even if the cell-phone is in the standby mode or turned 'off'.

[19] The Minister even acknowledged that the current voluntary arrangements are certainly satisfying: "Daarmee is [..] niet gezegd dat bestaande vrijwillige [..] arrangementen niet zouden voldoen. Het tegendeel is het geval." (Explanatory Memorandum 2007 30553 nr. 3).

7.5 Conclusion

In the Netherlands, the interference with the right to privacy for purposes of national security has a basis in law, the law is accessible to all, and the means of interference are sufficient foreseeable. Also the procedures specifying the balancing the interest of the protection of the national security with other interests of society, i.c. privacy, are adequate. Overall, adequate and effective remedies against abuse are available. That is, the remedies are effective to improve the overall performance of the AIVD. However, individuals with complaints on the AIVD cannot rely on an independent institute that can render legally binding decisions. Civil Dutch Courts may not decide fully informed, and those institutes that may be fully informed cannot render a legally binding decision (i.c. the Review Commission). Therefore, it is concluded that it is unlikely that the present Dutch remedy would pass as effective when a case would be brought before the ECtHR (cf. Cameron 2007, p. 57; Loof 2006, p. 833; ROB 2005, p. 46, see also Supreme Court in *Van Baggum*).

In addition, the Dutch definition or interpretation of the term national security is very broad and one should be careful that other issues will be dealt with using the umbrella of national security. However, the procedures to arrive at a decision to use special authorities to protect the national security are such that it is unlikely that the protection of the national security is misused for other purposes. It is therefore assessed that the procedures to balance national security and privacy for each operation are adequate. If these procedures are adhered to, a proper balance is likely to be established between privacy and national security.
Adequate procedures at the decision making level, however, do not guarantee compliance at the operational level. At the operational level several researches have found situations that may impact the balance between privacy and national security. One example is the inadequate data management (i.e. inappropriate requests, multiple requests for identical data, security of the infrastructure) throughout the security sector. The Review Commission proactively reviews the activities of the Security and Intelligence Agencies. The number of quality of the staff needs to keep pace with developments in the Security and Intelligence agencies to continue to fulfil the review task adequately.

At this moment, security seems to be the only value that needs to be addressed. Information from the AIVD is fully trusted and one commission has noted that there is little attention for organising counter forces (ROB 2005, p.56). It has been mentioned that society requires increasingly to shift the balance between privacy and national security to the latter. While (national) security seems to be a priority, privacy was an appendage of policy measures (see AIV 2006, p.37) and increasingly seems to become an appendage without any impact: the decision for a certain system are already made without seriously considering privacy-friendly options (see CBP 2006). Calls for the need to truly balance national security with other interests of society including privacy from a variety of respected institutes, commissions, or scholars (Data protection commission, AIV, Raad voor het Openbaar Bestuur, Rathenau Institute, Koops 2006) seem to be overwhelmed by the pressure to combat terrorism. Accordingly this call is ignored or denied by politicians resulting in increasing mandates for the security sector without justification other than we cannot afford to not have it; we have to fill the information gap; or bold statements like: increasing mandates and available means for Security and Intelligence agencies protects, instead of threatens, privacy. It does not provide arguments of why the current situation fails to comply with the terrorism threat, and if it fails this is because of the information gap (see also Koops 2006, p.37, 42; ROB 2005, p.44/46; Raad van

State 2005/6). Qualitative or quantitative data on how effective current means are, or how effective the new mandates may be, is not provided or initiated. For example, data on the number of taps in telecommunication was only provided once, in 2003, after significant effort from parliament to obtain these data. Unlike other countries, the security sector is not required to report these facts and accordingly cannot be held accountable for increases or decreases of the number of request for these data. This situation has resulted in non-informed decisions in parliament that may have shifted the balance between privacy and national security significantly. An evaluation of the effectiveness of used means is often lacking (Koops 2006, p. 37). This is unacceptable (ROB 2005, p.37 also referring to Raad van State's comments). In this respect, Canada's Privacy Impact Assessment (PIA) may be a best practice, enforcing government to consider privacy issues at the start of the decision-making process.
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.

Location data may be useful for purposes of national security. However, additional information is required for the execution of a security task. The interference with the right to privacy depends on a variety of factors: the use of the cell phone (active or standby mode), the level of detail of the location data (e.g., kilometres or 10 meter), the linkage with other datasets (the context), and the timeliness of the data (real-time v. data from last year).
These situation specific elements make it difficult to assess to what extent the use of location data interferes with the right to privacy. As a rule of thumb more detail is more sensitive than less detail, linkage to a wide variety of databases with personal data is more likely to interfere with the right to privacy than no linkages at all, and real-time data is more sensitive than older data. However, in specific instances the outcome of the balancing may be different.

8 The Netherlands: Balancing privacy and law enforcement

Location data of mobile devices can also be used for law enforcement purposes. The objectives of law enforcement and national security may compare with each other and sometimes overlap (see Van der Bel et al. 2007). Both are typical tasks of government and in addressing both objectives interferences with the right to privacy may arise. Location information may have a comparable role for both objectives: revealing links between people and events based on their location.
The balancing of law enforcement interests with privacy interests, including the use of location data, has been addressed in publicly available sources such as Court cases. These provide a more detailed overview of these matters than the information available on national security. In the context of this research, the information on law enforcement provides insights in the value of location data, and the way balancing law enforcement and privacy interests may be accomplished. We consider this useful insights for balancing national security and privacy.

8.1 Value of location information for law enforcement

In their research of the need of data retention for traffic data of telecommunications, Mul et al. (2005) found that in the Netherlands, traffic data of terminal equipment is considered an important instrument to reveal criminal 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), or to assess or confirm the reliability of an informant, although the legitimacy is disputed in the literature. Also location data may be used for verification purposes (Kamerstukken 2006-2007 nr. 31145 nr. 3 p. 9-10; Rotterdamse Politie 2003, p. 6 of appendix).
The identifying information of a cell-phone and the traffic information (who is calling who) are often more important for law enforcement than the location data. Location data of a cell-phone may be used to uncover a criminal network, but the other types of information can be more useful. For fraud research of historic traffic data is critical to reveal connections between suspects (Rotterdamse Politie 2003, p.5). Traffic data were already in 2003 found to be part of the standard procedures in law enforcement (Rotterdamse Politie 2003, p.5). In the instance of serious crimes such as murder, the responses to a survey in one research suggests that without historical traffic data approximately half of these crimes would not have been solved. For other crimes (organized crime, serious crimes) alternatives as more taps, requiring the traffic data earlier (*op voorhand vorderen*), more observations, and extending the time of research would have resulted in similar results (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). Objective of observation is to identify participants of a supposed criminal organization 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).
A beacon is only used in support of the dynamic observation means and serves only as a supportive means enabling to track an object at a certain distance. It is not an autonomous/ independent instrument in addition to the observation (HR 17 September 2002 LJN AE4200). For example, when an observation team follows a suspect and the team looses the suspect, the cell-phone data may bring them back to the suspect. In a robbery case, the police used the traffic data (location data) of the cell-phone to determine the escape route of the suspected device. Based on that information they found the murder weapon (see Court

Arnhem 30 July 2004 LJN AQ5858). Location data of a cell-phone is also valuable when an individual has been reported missing, e.g., kidnapping, or in a state of emergency.
Reijne et al. (1996) investigated through interviews with law enforcement officers, public prosecutors and judges (Magistrates), the value of phone taps as a law enforcement instrument. The research shows that a phone tap provides a quick and reasonable well picture of a criminal organization. In this respect it is not the content of the communication that is most interesting, but the contact information: who is calling who. Most interviewees see an advantage in using phone taps in combination with other investigative means, preferably with an observation team.
Phone call frequencies in that matter may be used to identify 'catch someone in the act' situations. In such instances the frequency of phone calls increases and because of stress also sensitive information may be revealed. Analysis of 95 criminal investigations shows that in approximately 50% of the phone taps provided indirect evidence, and in 36 cases it provided direct evidence. Phone call frequencies and content of a phone call are, however, difficult to compare with location information of mobile devices (Reijne et al. 1996).
The significance of the cell-phone in law enforcement might be increasing provided a quick scan on www.rechtspraak.nl with "mobiele telefoon" for 1999-2007 (1 in 1999, 37 in 2000, 41 in 2001, 82 in 2002, 103 in 2003, 146 in 2004, 176 in 2005, 254 in 2006, 252 for 2007).

8.2 Reliability of cell-phone data

Data from cell-phones are not by definition reliable law enforcement means. 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 (*peilzender*) does not domore 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, in chapter 6, it is explained that it is not necessarily the nearest BTS that is 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. In (Court Amsterdam 20 April 2006 LJN AW2513) the court ruled, although the cell-phone of the victim used BTS tower A and the cell-phone of the suspect did use BTS tower B 20 minutes later, and the BTS-s were only 300 meter apart, this was insufficient to evidence the relation that the suspect was the murderer. Thus, 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.

The Supreme Court holds that if the subscriber of the cell-phone does not dispute that the phone was in his possession at the time of the crime, it is assumed that he was the user of the cell-phone located at the crime scene (HR 5 June 2007 LJN BA1024; Court of Appeal The Hague 29 June 2004 LJN AQ1112). Also if the subscriber cannot explain who else might have used the suspected device at the time and location of the act, it is assumed that

the subscriber is the user (see HR 7 September 2004 LJN AO9090). In the instance that the cell-phone was found on the suspect at the moment of 'arrest', several minutes after a critical phone call was made, it was assumed that he was the user (Court Haarlem LJN AX9578). In another case, the suspect used the EMEI-code (the phone) of the stolen cell-phone in combination with his own IMSI-code (code linked to the phone number). Since he called several identical numbers before and after the robbery with the same IMSI-code but with a different EMEI-code he was assumed to be the user of the stolen phone (Court Maastricht LJN AZ8384). Also in the instance of a kidnapping, the victims had stressed that the suspects used their cell-phones at the time of the kidnapping. Based on the location and the time of the kidnapping, the used phones could be identified, and a tap on these phones resulted in the arrest of the suspects (Court of Appeal in The Hague LJN AQ1112).

8.3 Balancing law enforcement needs with privacy

In chapter 3, we developed six principles to which personal data processing should adhere to. These principles are:

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.

Principle 5: guaranteed accuracy of the data for the purposes of use.

Principle 6: individual participation in the process whenever possible.

In this section, we will provide for each principle an assessment of the extent to which the Netherlands for law enforcement adheres to these principles.

8.3.1 Principle 1: interference for law enforcement 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 Netherlands, the Data Protection Act (*Wet bescherming persoonsgegevens* (Wbp)), the Act on Judical and Criminal Proceedings Data (*Wet justitiële en strafvorderlijke gegevens*) and the Telecommunication Act (Tw) provide the framework for the data processing for all purposes except for purposes of national security and preventing, tracing and prosecuting criminal acts. For the latter, a legitimate basis for interferences of the right to privacy for law enforcement purposes can be found in the Code on Criminal Proceedings (*Wetboek voor Strafvordering*), the Police Act (*Politiewet*), and the Act on special authorities for law enforcement (*Wet bijzondere opsporingsbevoegdheden* (Wet BOB)).

Transparency of the means available to law enforcement
The means available to law enforcement are specified in the Police Act, Code on Criminal Proceedings. More specifically, the Act on special authorities for law enforcement, Decree Technical Means Supportive to Criminal Proceedings (*Besluit technische hulpmiddelen strafvordering*), Act on the police registers (*Wet op de politieregisters*), the Decree police registers (*Besluit politieregisters*), Decision powers of criminal investigation (*Aanwijzing opsporingsbevoegdheden*), and Act on local government (*Gemeentewet*), among others, provide what means are available for law enforcement. Other relevant legislation are the Decree Security Data Tapping Telecommunication and the Act on Secret Surveillance through Camera's (*Wet heimelijk toezicht camera's*).

Transparency in what data can be claimed
The Code on Criminal Proceedings, Act Requisition Telecommunication Data, Decree Requisition Telecommunication Data, Decree Dissemination Telecommunication Data, Decree Special Acquisition Phone Numbers, and the Telecommunication Act specify what data can be claimed. All telecommunication data (i.e., identifying data, traffic data, and location data) can be claimed depending on the (seriousness of the) suspicion.

The Code on Criminal Proceedings (*Wetboek van Strafvordering*) distincts now six categories of data, each with separate regimes (from least sensitive down to most sensitive for which stricter regime applies):

- identifying data (data that determine the identity of individuals and that connect people and situations: name, address, sex, birth date, administrative characteristics such as phone number, bank account number, client number, license plate number);
- user data;
- traffic data;
- certain stored data (e.g., location data of cellphone in standby mode);
- certain stored data that are processed after the requisition date and need to be directly provided to law enforcement;
- sensitive data (data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or concerning health or sex life and data in the category of the letter and phone secret (*brief en telefoongeheim* art. 13 of the Dutch Constitution).

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

The more precise the suspicion, and the more serious the criminal act, the higher the societal interest to solve the crime and the more legitimate an infringement of the right to privacy (HR 12 February 2002 LJN AD9222; see also Nouwt et al. 2004, p.336). If a privacy infringement is assumed, then the Supreme Court accepts a light legal basis as sufficient for meeting the 'in accordance with the law' requirement (Buruma 2001, p.35). Generally, suspicion of a serious crime (carrying at least a maximum of four years detention), participation in criminal organisation, or terrorism are sufficient to use special authorities. For the most infringing means it is required to have a suspicion of a serious crime that has a major impact on public order, participation in criminal organisation with a major impact on public order, or terrorism. In addition, these can only be used if the investigation requires this urgently.

In balancing privacy and law enforcement relevant aspects are: the consecutive period of observation (hours, days, weeks), the intensity (continuous, periodic or with intervals) and frequency, the (intimacy of the) place (public road, home, office), the objective of the observation, the way the observation is accomplished (technical means as camera's or beacons and their possibilities), the urgency of the investigational need, the inconvenience for the observed person, and the degree of suspicion of the observed person (see Buruma 2001, p.36; Mevis 2001, p.66/91; Kamerstukken 98-99 25403 nr. 25, p.5; Kamerstukken 97-98 25403, nr. 7, p.47; Kamerstukken 1996-97 25403 nr. 3, p.27; Supreme Court 21 March 2000 LJN AA5254; Supreme Court 12 February 2002 LJN AD9222). The longer the period of observation, the more intimate the place of observation, the higher the intensity or frequency of observation, and the more possibilities the supportive means provide, the higher the chance that an almost complete picture of a part of someone's private life will be obtained (Kamerstukken 1996-97 25403, nr. 3 p.27). The tapping of cell-phones is a far-reaching means to use in law enforcement and can only be used if there is a serious infringement of the system of law (Kamerstukken 1996-97 25403 nr. 3, p.23). The use of an IMSI-catcher is regarded as the technically most advanced means to use. It can only be used with consent of the responsible Minister on request of the public prosecutor (art. 13.4(1) Tw).
The procedure to use a special means, e.g., tapping a cellphone, is as follows. First, the law enforcement officer creates a report (*proces-verbaal*) explaining why a special means is necessary. This report, together with a standard form, is provided to the public prosecutor. If the public prosecutor agrees, he signs the request and both documents are submitted to the Magistrate for approval. When approval is obtained, the public prosecutor orders law enforcement to use the special means. Law enforcement then claims the data from the telecom providers, and finally the data is provided.
Balancing different interests of society takes place in five instances: with the initial report, in the public prosecutor, the Magistrate (*rechter commissaris*, an especially appointed judge), in the specialised services of law enforcement executing the request and ultimately in court (if applicable). For identifying and traffic data, the Magistrate's approval is not required.

Nouwt (et al. 2004) refers to the Supreme Court case on evidence obtained from permanently installed cameras that the cameras were covering areas in public space, where the suspect had no reasonable expectation of privacy. There was no true interference with the right to privacy due to the limited time the suspect and his accessories had been observed. The purpose of preventing disorder in public spaces was judged to be legitimate, and the placement of the camera was in accordance with a legitimate procedure.
In the Dutch Supreme court judgment of *Zwolsman*, the court has ruled about the legitimate eavesdropping of cell-phones. It notices that users of cell-phones should accept a limitation in their expectation of privacy when using such a device since it is generally known that it is technically relatively easy to 'tap' cell-phones. However, if the tapping is 'on purpose' and for a consecutive period of time (i.c. three weeks), article 8 ECHR applies. In this instance, a legitimate basis is required under article 8.2 ECHR. The Police Act of 1993 did not provide the legitimate basis required under art. 8.2 ECHR. Therefore, the Court ruled a violation of art. 8 (CBP 2004, p.32). Further, the Court ruled that since the tapping was only for three weeks, only one side of the conversation was eavesdropped, the specified purpose of the eavesdropping, and the use of the "scanners" was ineffective, the invasion of the privacy was not sufficiently enough to hold the public prosecutor non-admissible (*niet-ontvankelijk*) in its criminal procedure (CBP 2004, p.32).
In instances of missing people or kidnappings, the Code on Criminal Proceedings does not apply since the cell-phone that is the object of investigation does not belong to a suspect but to the (potential) victim. Thus, the Data protection act applies and it is the telecom provider

that has to be convinced that the processing is necessary in order to protect the vital interests of the data subject (art.7(d) 95/46/EC; art.8 (d) Wbp). A similar situation may arise when there is information that someone is going to be killed at a certain location and time. Location data of the cell-phone of the potential victim may then confirm the reliability of the information and safe the life of the potential victim.
In the 2004 case of a girl kidnapped by someone detained under a hospital order, it was not allowed to track his mobile phone (Kamerstukken 29452, nr. 6) because he was not a suspect of a criminal offence. Later when his personal data were linked to a stolen car, he became a suspect and could be tracked. Based on this case the Minister announced new powers for law enforcement (see Kamerstukken 29413), which became law on 1 July 2005.

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

The subsidiary criterion
Table 8-1 provides some insight in the different regimes for different types of data. For identifying and user information the requirement is that it should concern a suspect of crime, organised crime or terrorism. Traffic and location data (historic or future) of telecommunications can be requisited by the public prosecutor for investigative research[20], i.e., indications of serious crimes; investigations of committed crimes or pro-actively addressing organised crime through identifying criminal networks (Sietsma 2007, p.38); or investigations on terrorism.
Sensitive data processing requires the highest authority (the Magistrate) to consent. The highest authority consent requirement also applies to the content of communications (email, voice mail, phone tap), and the real-time (location) data of cell-phones (see Table 8-1).
For the real-time tracking and tracing of individuals the Magistrate not only needs to confirm the urgency for the use of such means, but also whether this would not demand an unreasonable effort for the telecom provider (Explanatory Memorandum Kamerstukken 2003-2004, 29441, nr. 3 p.9). Therefore, these means should be used to the minimum extent possible (only in very urgent instances) (Explanatory Memorandum Kamerstukken 29441, nr.3 p.25). Mevis (2001, p.66, p.91) holds that the public prosecutor misuses his powers when he demands special efforts from telecom providers if he can arrive at similar results with the special authorities available to him such as 'physical observation'. Only if such data cannot be reasonably collected through these means and a pressing investigative need is present, the monitoring may be accomplished through the cell-phone data.
The order of sensitiveness in Dutch law (Sv) may be as follows (from most sensitive down):

- sensitive data; content of the communication (conversation; email/ voice mail), real-time (location) data;
- (historical and future) traffic and location data (standby or active use);
- user data, and identifying data.

The Minister has argued that the registration of images or movements of individuals with a technical means is more far-reaching than the observation of images or movements by an observer who reports the movements ex-post. A registration makes it possible to process at any time an exact and complete picture of what is being observed. It further allows for

[20] Location data can be requisited for those suspicions of crimes as described in art. 67 Code on Criminal Proceedings (for which a 4 year detention penalty applies and other more serious criminal acts).

searches specifically focussing on a certain time and place (Explanatory Memorandum wet BOB Kamerstukken 1996-1997 25403, nr. 3, p. 27, referred to in Buruma 2001, p. 43).

Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij (Mevis commission, 2001) (Commission Data Collection for Criminal Proceedings in the Information Age)

Provided developments in information and communication technology, the *Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij* (Mevis commission) was asked in 2000 by the Minister of Justice to investigate the extent to which the Code on Criminal Proceedings provided an adequate legal framework for those (new) means of data collection and processing necessary for criminal proceedings. The commission supervised by P.A.M. Mevis recommended to introduce in the Dutch Code on Criminal Proceedings different regimes for different types of data. It distinguished the content of the communications, traffic data, identifying data, and other data, and identified the difference between historical data and realtime data. Most of their recommendations were introduced in the current Code.

The proportionality criterion

For the proportionality criterion, interviewees indicated that it is difficult to provide a general decisional framework to assist in the balancing of law enforcement and privacy since each case is unique; the standard case does not exist. Therefore, what may be proportionate in one case, might be disproportionate in another. Several examples may clarify this.

1. A series of purposely lighted fires in Amsterdam may not have a great impact on the public order as a similar series in a small town.
2. A marihuana plantation in a villa may be something else than a marihuana plantation of a similar size in a small apartment in the centre of a town, where also energy is illegally tapped and neighbours complain about smell and water nuisances.
3. A woman complains that she is being stalked by someone frequently calling her number. It appears that this concerns her ex-husband calling her to stop harassing him.

In each of the cases different means may be applied for apparently a similar offence. Another example is in the following situation. A description of a suspect is developed and based on this information cell-phone data of the suspect might be tapped and historical data requested. The AIV (2007, p.80) refers to Jacobs with noting that previously first possible suspects were selected and then additional information about them was collected. Now first a huge amount of data on innocent citizens is processed and then attempted to find the most likely suspect (translation BVL). One interviewee argues that it is unjust to first request data on all cell-phones in the neighbourhood at the time of a committed crime and based on this information go after the subscribers of the cell-phones. Other interviewees find such an approach useless for law enforcement since it provides very much (irrelevant) information, also from cell-phones several kilometres away. However, if no other means are available, it can be used (see LJN AQ1112 Court of Appeal The Hague).

Many would not realize that with a tap for a consecutive period of time a complete picture of someone's life can be obtained. It may provide much more detailed information on someone than a house search. However, for a search warrant (*huiszoeking*), interviewees indicate that it will be much more difficult to obtain approval from the Magistrate. One of the interviewees

argues that for a phone tap a similar strict regime as for a search warrant should apply. Similarly, one may wonder why a search of a shed or the secret observation at a market requires higher authorities to approve and stricter procedures than systematic observation (Buruma 2001, p. 42).

The number of taps that are executed on a daily basis, 1681 taps (Minister of Justice 2008), suggests that either a significant part of law enforcement is involved in the tapping business, or that a significant part of these taps is placed without being used. The latter situation would imply a disproportionate interference with the right to privacy.

For telecommunication data the extent to which the proportionality criterion is being adhered to may be questioned. Concerning telecommunications data, a public prosecutor typically does not specify what data can be processed from a cell-phone tap. A typical order, to which the Magistrate consents, includes all data that is processed in telecommunication: the content of conversations, identification data, traffic data and location data. Together, these data may have a greater interference with the right to privacy than only one aspect of the telecommunications data. It may very well be that the use of only one type of data is sufficient to fulfil the law enforcement task. The proportionality requirement is in such instance inadequately fulfilled.

Type of data (Wetboek van Strafvordering)[21]	Examples	To be used if suspicion of:	Decision/ Requisition by/ (reported by)	Max. period requisition (+ ext)	Sv article
Identifying data	Name, address, sex, birth date, administrative characteristics[22]	Crime, organised crime with major impact on public order, or terrorism	Law enforcement officer (Law enforcement officer reports)	-	126nc; 126uc; 126zk;
User data[23] [24]	Name, address, phone number (MSISDN), IMSI code, EMEI code, and type of service used[25]	Crime, organised crime with major impact on public order, or terrorism	Law enforcement officer (Public Prosecutor reports)	-	126na; 126ua; 126zi;
Traffic data[26] [27]	Historic traffic data (including location data of cell-phone if actively been used) (incl. date and time of use); and future traffic data	Serious crime[28], organised crime with major impact on public order, or terrorism	Public Prosecutor (Public Prosecutor reports)	3 months (extension possible)	126n; 126u; 126zh;
Certain stored data: other data	location data of cell-phone if in standby mode[29]	Serious crime, organised crime with major impact on public order, or terrorism	Public Prosecutor (Public Prosecutor reports)	-	126nd(1) via 126ng(1); 126ud(1) via 126ug(1); 126zl(1) via 126zo(1)
Certain stored data processed after requisition date	location data of cell-phone if in standby mode	Serious crime, organised crime with major impact on public order, or terrorism	Public Prosecutor (Public Prosecutor reports)	4 weeks (+ 4 weeks)	126ne(1) via 126ng(1); 126ue(1) via 126ug(1); 126zm(1) via 126zo(1)
Certain stored data: other data	location data of cell-phone if in standby mode	Other criminal fact than serious crime	Magistrate (Public Prosecutor reports)	4 weeks (+ 4 weeks)	126nd(6)
Certain stored data processed after	Real-time location data of cell-phone;	If the investigation of serious crime, organised	Magistrate	4 weeks (+ 4	126ne(3) via 126ng(1);

[21] In the Netherlands only art. 126n and 126na Sv are commonly used.
[22] Administrative characteristics are characteristics that relate the suspect and a third party to whom the data requisition is directed, or the characteristics of the services provided to the suspect. These may be membership number, number of an insurance, bank account number or client number (Kamerstukken 2003-2004, 29441, nr. 3, p.7)
[23] See Wet bijzondere opsporingsbevoegdheden (§ 2.3.4)
[24] See Besluit verstrekking gegevens telecommunicatie
[25] Type of service refers to speech, fax, SMS, MMS, WAP, GPRS, among others (see Stratix 2003, p.23, 38)
[26] See Wet bijzondere opsporingsbevoegdheden
[27] See Besluit vorderen gegevens telecommunicatie
[28] Serious crime is in this context a crime for which preventive custody (*voorlopige hechtenis*) can be executed (see www.zakboekenpolitie.com).
[29] Since Dutch telecom providers do not store standby data. These data are not claimed by law enforcement.

requisition date and directly (or each time within a certain period after processing) available to law enforcement	real-time financial transfers	crime with major impact on public order or terrorism requires this urgently	(Public Prosecutor reports)	weeks)	126ue(3) via 126ug(1); 126zm(3) via 126zo(1)
Sensitive data	Data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or concerning health or sex life	If the investigation of serious crime with *major impact on public order*, organised crime with major impact on public order or terrorism requires this urgently	Magistrate (Public Prosecutor reports)	-	126nf(1/3); 126uf(1/2); 126zo(2/3)
Content of communication	Conversation	If the investigation of serious crime with *major impact on public order*, organised crime with major impact on public order or terrorism requires this urgently	Magistrate (Public Prosecutor reports)	4 weeks (+ 4 weeks)	126m; 126t; 126zg;
Content of communication	Email/ voice mail[30]/ SMS from, meant for, or concerning the suspect or the criminal fact	If the investigation of serious crime with *major impact on public order*, organised crime with major impact on public order or terrorism requires this urgently	Magistrate (Public Prosecutor reports)	4 weeks (+ 4 weeks) (from interviews)	126m 126ng(2); 126ug(2); 126zo(2);

Table 8-1 Special means regimes for law enforcement

[30] EK 2004-2005 29441 E, p.4; Kamerstukken2004-2005 24991, nr.3 p. 14; see Stcrt 16/10/2006, nr. 201 p. 14

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

For each requisition of telecommunication data, a official report (*proces-verbaal*) is created in which (ex-ante) the decision to use a special means is justified. The law enforcement officers should do this for the requisition of identifying data, the public prosecutor for all other data. Directly after the requisition, stakeholders can file a complaint with the Court (*rechtbank*, art. 552a Sv). Further, there is an ex-post assessment by the criminal judge in the instance of prosecution. In addition, the Supreme Court (12 February 2002 LJN AD9222) has stressed that a judge cannot be expected to accomplish further research into satisfaction of the requirements of proportionality and subsidiarity of art. 8(2) ECHR, other than a check whether the legal requirements are satisfied, and the judge has confirmed that the Magistrate in all reasonableness has come to a judgment that the proportionality and subsidiary requirements were satisfied (at 73) (translation BVL).
Abuse of the data processing rules can be punished. The Dutch Penal Code (art. 139a WvS) has penalties with a maximum penalty of imprisonment for 6 months for those in law enforcement abusing their legal mandates.

8.3.5 Principle 5: guaranteed accuracy of the data for the purposes of use.

The Act on Judicial and Criminal Proceedings Data (Wet justitiële en strafvorderlijke gegevens) requires that the data need to be accurate for the purposes of use (art. 39).
In their assessment of the security of the tapping systems of the interception organisation (tapkamers) PriceWaterhouseCoopers (2003) concluded that the technical security (authorization) for use of the data in the system was insufficient (e.g., non-specific authorizations, non documented access, no encrypted communications, no back-ups, no information security policy). One specific issue was the inability in one of the interception organisations to remove the data that was gathered through a tap order when the case has been finalised. Thus, even if the Public Prosecutor has ordered to delete the data, the data remained accessible (Price WaterhouseCoopers 2003, p.20). In 2007, research accomplished by the Dutch Data Protection Agency (CBP) found that data from taps that concerned communications with individuals (e.g., lawyers) for which the right of non-disclosure (verschoningsrecht) applies were, contrary to the law, not always deleted (in-time) (CBP 2007).

8.3.6 Principle 6: individual participation in the process whenever possible.

On request, individuals must be provided with information about their judicial and criminal proceeding records (artt. 18, 39j, 39m Act on Judicial and Criminal Proceedings Data). Individuals have the right to correct or add personal data.
For serious crimes the records on Criminal Proceedings need to be removed after thirty years. For minor crimes these need to be removed after five years.
Since 2003, with the Wet BOB, suspects have to be informed that their telecommunication were being tapped[31]. The evaluation of the Special authorities act indicated that this notification obligation was only been adhered to at a very limited scale, however (see Kamerstukken 29940, nr. 4, p. 1).

[31] The Wet BOB specifies transparently which means may be used in what instances, among others.

8.4 Developments in Law enforcement

Several developments have pushed the balance between privacy and law enforcement towards the latter. Since 1 February 2007, law enforcement agencies can apply special powers (including tapping telecommunications) if there are indications of involvement in an act of terrorism or other severe criminal acts (see Stb. 580; Kamerstukken 30164). This is a lighter requirement than the previous required suspicion or reasonable suspicion of involvement in such acts (cf. US for similar developments in Levi et al. 2004, p.204).
Since 1 January 2006 (Stb 609, 2005; Stb 390, 2005; Kamerstukken 29441), the Telecommunication Act (art. 13.2b) and the Code on Criminal Proceedings (art. 126nc-126ni and 126uc-126ui) require providers of telecommunication networks and services to obey requests of law enforcement agencies (such as police) for certain stored or registered identifying data. This may not have been necessary since especially telecom providers almost always provide the requested data to law enforcement (Mul et al. 2005, p.18).
Since 1 July 2005 (Stb. 105, 2004; Stb. 311, 2005), the Telecommunication Act (art. 13.2a) and the Code on Criminal Proceedings (Sv, art. 126n and 126 u) require providers of telecommunication networks and services to provide for specific crimes the public prosecutor on request data concerning a user and the telecommunication traffic with regard to this user.
In December 2003, the Minister acknowledged that for law enforcement purposes location data could only be used for tracking if the user communicates 'actively'. He concluded that the ability to also track someone when the cell-phone is on stand-by, this would be a severe intrusion of the right to privacy, similar to continuous observation of individuals. The Minister decided that such deviation in the use of the data is undesirable (Kamerstukken II 2003-2004, nr. 28059 A, cf. Decree Requisition Telecommunication Data, art. 2e). However, two years later it was decided that law enforcement agencies are allowed to track on a continuous basis those involved in or suspected of severe criminal activities (Code on Criminal Proceedings art. 126ng/ug & art. 126ne/ue, see also Stcrt. 16/10/2006 nr. 201, p.14).

Requests for data have strongly increased over the years and it seems that this development will not end in the near future (AIV 2007, p.70). The AIV suggests that intelligence and law enforcement agencies unlawfully request data without respecting legal obligations of proportionality and subsidiarity tests. For example, the financial sector has reported 180,000 unusual transactions (e.g., transactions over 10,000 euro). Only 130 cases were, however, brought to court (less than 0.1%) (AIV 2007, p.74).
Interviewees indicate that the phone tap is the most used special BOB authority in law enforcement. Some interviewees indicate that since the new Wet BOB public prosecutors may easier use the tap authority. Before, they were more uncertain about the appropriateness of using the tap authority and were more likely to better balance such a decision with privacy considerations and alternative means. In this respect, the new law may have resulted in a devaluation of considered decisions. Other interviewees, however, disagree with this suggestion.

Implementation Data Retention Directive

Through data analysis, location data can also be used to find users of unregistered phones, such as pre-paid phones. For this reason, the telecom providers in the Netherlands are required to store data concerning the time of communications, the numbers corresponding with the time and telecommunication, and the BTS through which the communication was facilitated (Besluit bijzondere vergaring nummergegevens telecommunicatie, Stb. 2002, 31). Based on this Decree the location data are stored for three months. In the Explanatory Memorandum of the Implementation of the Data Retention Directive, the Minister confirmed that the data storing requirement was not for law enforcement purposes (Explanatory Memorandum Kamerstukken 2006-2007

31145 nr. 3, p. 9-10). However, four sentences later in the same document the Minister notes that government agreed with the Decree because it allows to identify unregistered users of cell-phones for law enforcement purposes (referring to Kamerstukken 1997/98 25533, nr., 8, p.11). The proposed Dutch implementation act of the Data Retention Directive requires telecom operators to store all traffic data in telecommunications for 18 months. Supportive information why it is necessary to store the data longer than the required minimum of six months is lacking, however.
One of the expected results of the implementation of the Data Retention Directive (2006/24/EU) is an increase of requests for telecom and internet data (see Explanatory Memorandum Wetsvoorstel bewaarplicht telecommunicatiegegevens Kamerstukken 2006-2007 31145) of 20% (see AIV 2007, p.44 referring to Kamerstukken 2006-2007 and Verdonck et al. 2006). However, based on the provided information in the Explanatory Memorandum on the cost aspect one may expect an increase of 75% (see Explanatory Memorandum 31145, nr.3).

8.5 Balancing law enforcement with privacy interests

In the Netherlands, the interference with the right to privacy for purposes of law enforcement has a basis in law, the law is accessible to all, and the means of interference are sufficient foreseeable. Also the procedures specifying the balancing the interest of law enforcement with other interests of society, i.c. privacy, are adequate. Overall, adequate remedies against abuse are available. They are, however, not always effective.

Balancing aspects
Court rulings and discussions in parliament have provided a well-developed framework for balancing privacy and law enforcement needs. These considerations may very well apply as well to the balancing of national security and privacy. In balancing privacy and law enforcement relevant aspects are: the consecutive period of observation (hours, days, weeks), the intensity (continuous, periodic or with intervals) and frequency, the (intimacy of the) place (public road, office, home), the objective of the observation, the way the observation iss accomplished (technical means as camera's or beacons and their possibilities), the investigative urgency, the inconvenience for the observed person, and the degree of suspicion of the observed person. The longer the period of observation, the more intimate the place of observation, the higher the intensity or frequency of observation, and the more possibilities the supportive means provide, the higher the chance that an almost complete picture of a part of someone's private life will be obtained. The tapping of cell-phones is a far-reaching means to use in law enforcement and can only be used if there is a serious infringement of the system of law.

Telecommunication data
There are several types of data that are part of the general telecommunications data pallet: the content of the communication, identifying data, traffic data and location data. Also difference is made between historical, real-time and future location data. Several observations may question the extent to which requests for telecommunication data adhere to the proportionality criterion. Concerning telecommunications data, a typical order to which the Magistrate consents, includes all data that is processed in telecommunication: the content of conversations, identification data, traffic data and location data (if available). Together, these data may have a greater interference with the right to privacy than only one aspect of the telecommunications data. It may very well be that the use of only one type of data is sufficient to fulfil the law enforcement task. Public prosecutor and Magistrate should be aware of the different types of telecommunications data and be sensitive to the privacy impact of requiring all types of telecommunication data.

Transparency of the law

The increased transparency of the law, fully adhering to the requirements of the ECtHR may have resulted in an increased use of the most privacy interfering means. One may conclude that the more vague legislation is on the use of certain means interfering with human rights, the less interferences with these rights are sought or agreed with. It would be beneficial if this suggestion is backed with factual evidence. However, such data was lacking in the Netherlands since the Minister did not find it useful to collect. On 27 May 2008, the Minister revealed that for law enforcement 12,491 tap orders were provided for the second part of 2007 (Minister of Justice 2008). These concerned 10,490 (84%) cellphone numbers. On each day, on average 1681 taps were active.

Economics protecting privacy

Another observation is that the operations of the telecommunication providers aiming at cost effectiveness, are currently to a great extent safeguarding privacy. Standby data of cellphones is typically not stored due to the costs associated with it. Also location data, being more detailed than traffic data, is typically not stored. However, the increase of the coverage of the telecom network may question the difference between location data and traffic data. Strictly taken, the EC 2002/58 only data necessary for the billing purpose of a telecommunication needs to be stored. In the Netherlands, this billing information would generally only require that the call was from within or outside the Netherlands. More specific information, i.e. information on use of BTS, is not necessary for billing purposes. The development is, however, that the traffic data is becoming more detailed as apposed to less detailed. In addition, in the European Union, it has been the implementation of the Data Retention Directive that requires the retention of traffic data.

Improving effectiveness of current means

Currently, a phone tap or the requisition of traffic data is based on the unique characteristics of the cell-phone (i.e., IMSI, phone number, IMEI). No other communication means than the ones described in the warrant can be tapped.

From the perspective of law enforcement, it may be worthwhile to consider to introduce a system that for tapping or requesting cell-phone data of a specific individual instead of requiring data from a specific object (i.e. the cell-phone). Suspects may change frequently their cell-phones, sometimes every day. For each of the cell-phones a separate warrant needs to be provided. It appears impossible to approve taps at this same pace so that they may always be several steps behind the suspect.

One of the arguments used in explaining the significant growth of phone taps is the number of communications means used per citizens. Through allowing a tap on communication means used by a suspect, independent from the number of communication means a more objective assessment of the number of taps can be acquired. Further, in a tap warrant the telecom provider needs to be specified. It is not allowed to have a general warrant that applies to all telecom providers. This seems to be overly restrictive.

9 Canada: balancing privacy and national security

This chapter focuses on the way privacy and national security interests are balanced with respect to the use of location information of mobile devices for national security purposes. First, it addresses how privacy as a general concept is considered in Canada. The reasonable expectation of privacy doctrine is central in this section. In the second section, Canadian national security is addressed and some practical information on surveillance provided. In section 3, the balancing of national security needs with privacy is assessed through the balancing principles developed in chapter 3. In section 4, the main findings on balancing are summarized. Finally, conclusions are presented in section 5.

In 2007, Canada has approximately 33.5 million people spread over an area of 9,984,670 sq km (worldfactbook 2008). Canada is a member of the United Nations and the OECD.

9.1 Privacy in Canada

Canadian privacy law has been qualified as a comprehensive regulatory model with a public official in charge of enforcing data protection legislation (Beresford 2005, p.34). Privacy legislation in Canada has been assessed by Privacy International & EPIC as one with significant privacy protections and safeguards for almost every researched aspect (including constitutional protection, statutory protection, privacy enforcement, democratic safeguards, leadership and communication's data retention) (Rotenberg et al. 2006). For communication's data retention it was considered to have no invasive policy or widespread practice/ leading in best practice. In the 2007 rankings of the Privacy International and EPIC Privacy Survey, Canada has decayed from an overall 'significant protections and safeguards' qualification to a 'some safeguards but weakened protections' status (Privacy International et al. 2007). The individual decreased scores on privacy enforcement, ID cards and biometrics, and surveillance of medical, financial and movement may be causes for the poor overall score.

Canada's Charter of Rights and Freedoms (Section 8: "Everyone has the right to be secure against unreasonable search or seizure") may be regarded as the constitutional basis to protect the right to privacy. The values underlying the privacy interest protected by Section 8 are dignity, integrity and autonomy (*R. v. Plant* 1993). In addition, in *R. v. Edwards* (1996), the Court ruled that the right to be free from intrusion or interference is a key element of privacy. It protects a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This includes information which tends to reveal intimate details of the lifestyle and personal choices of the individual (*R. v. Plant* 1993).

Also section 7 of Canada's Charter, which guarantees 'the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice', encompasses aspects of privacy interests. Such rights are for example related to physical or psychological integrity or the right to independently make basic personal choices (O'Connor 2006, p.433).

The Charter protects people against unjustified government intrusions upon their privacy. The degree of protection depends on the reasonable protection of privacy of the individual in the circumstances (R. v. Wise; Young 2007). The expectation is based on what privacy people reasonably can expect in a free and democratic society (*R. v. Wong*; Nouwt et al. 2004, p.352). In *R. v. Duarte* the Federal Court explained it as follows:

> "A reasonable expectation of privacy demands that an individual may proceed on the assumption that the state may only violate this right by recording private communications on a clandestine basis when it has established to the satisfaction of a detached judicial officer that an offence has been or is being committed and that interception of private communications stands to afford evidence of the offence.[..] Where persons have reasonable grounds to believe their communications are private communications, the unauthorized surreptitious electronic recording of those communications is an intrusion on a reasonable expectation of privacy."

The Canadian reasonable expectation of privacy does not distinguish between people's activities (criminals do have the same privacy expectation as anyone else). The activities of the person potentially subject to an infringing measure are not central, but the infringing activity is (*R. v. Tessling; R. v. Wong; Hunter*).

Determining a reasonable expectation of privacy

A reasonable expectation is to be determined on the basis of the totality of the circumstances (*R. v. Edwards*). *R. v. Tessling* categorized three types of privacy where a reasonable expectation of privacy exists: (1) privacy of the body, (2) territorial privacy, and (3) informational privacy. The latter two may refer to location privacy.

Territotial privacy concern the location where the activity took place. A greater degree of privacy may be expected in a private place such as a home, office or hotel room than in public areas, commercial buildings, or a car (see Canadian Charter of Rights Decisions Digest 2004; see also *R. v. Wong*, *R. v. Wise*). Although the place where a search occurs greatly influences the reasonableness of the individual's expectation of privacy (*R. v. Tessling*), it is not determinative (*R. v. Wong*); the Charter protects people, not places. For example, in *R v. Tessling*, the Court ruled that information obtained from a camera flying over property measuring heat generated by a house could not permit any interferences about the precise activity in the house, did not touch on a biographical core of personal information, nor did it tend to reveal intimate details of a lifestyle. Therefore, taken the totality of the circumstances, showing that some activities in the house generated heat, no privacy interference was found. It was not relevant that this general, meaningless [no differentiation between one source or another was possible] information could not be observed from the outside with the naked eye (*R. v. Tessling*).
Although in public places, such as stores, and restaurants one does not expect solitude and total freedom of observation, equally one does not expect to be under secret surveillance (Westin 1967, p.112). Therefore, a lower expectation of privacy does not imply that one does not have any human right protection.

For a property search, an interference with the most intimate territorial expectation of privacy, *R. v. Edwards* considered in its assessment of a reasonable expectation of privacy:

(1) the presence at the time of the search;
(2) possession or control of the property or place searched;
(3) ownership of the property or place;
(4) historical use of the property or item;
(5) the ability to regulate access;
(6) the existence of a subjective expectation of privacy; and
(7) the objective reasonableness of the expectation.

With respect to informational privacy, *R. v. Plant* (1993, p.16) considered in its assessment of the expectation of privacy:

(1) the nature of the information itself;
(2) the nature of the relationship between the party releasing the information and the party claiming its confidentiality;
(3) the place where the information was obtained;
(4) the manner in which it was obtained and the seriousness of the crime being investigated allows for a balancing of the societal interests in protecting individual dignity, and
(5) integrity and autonomy with effective law enforcement.

R. v. Tessling further developed informational privacy as being information about a person's activities. This includes information about the home (size, heat generation, colour front door), and the quality of the information (content, level of detail). It applies to what is happening inside the home; what interference can be drawn about the activity going on in the house?
It was argued that a conversation with an informer does not amount to a search and seizure within the meaning of the Charter; it is not meant to protect against a poor choice of friends. Electronic interception and recording of private communications [the conversation] does amount to a search and seizure (*R. v. Tessling*).
In New Foundland the Supreme Court found a substantially greater expectation of privacy concerning one's financial information and transactions on one's bank account than for one's electricity consumption ([1994] N.J. No. 142, see also *R. v. Plant*). In *R. v. Weir* the Supreme Court found for unencrypted email a lower expectation of privacy than for encrypted email or first class letter mail since unencrypted mail is vulnerable to being read by unintended third parties (Young 2007, p. 53).
Informational privacy may include information on one's movement. Concerning the expectation of privacy in one's movements, *R. v. Wong* referred to Orwell's 1984 where citizens had every reason to expect that their every movement was subject to electronic video surveillance. This contrast with the expectation of privacy in a free and democratic society "could not be more striking" (*R. v. Wong;* see also *R. v. Wise* dissenting opinion of La Forest J.). Thus, there is generally a reasonable expectation of privacy in (information on) one's movements.

9.2 National security in Canada

In the 1970s, Canada dealt with a violent separatist movement in Quebec that was assessed as a very dangerous threat to Canada's public safety (Filmon 2007). Another major event was the 1985 Air india Flight 182. The airplane exploded through a bomb, killing 280 Canadian citizens.

Many federal organisations have national security responsibilities. These include the Canadian Security and Intelligence Agency (CSIS), Royal Canadian Mounted Police (RCMP), Canada Border Service Agency, Communications Security Establishment Canada (CSEC), Department of Justice, Canadian Air Transport Security Authority, Health Canada, Public Safety and Emergency Prepardeness Canada, among others (O'Connor 2006, p. 127). CSIS is the primary focus of this research. Where applicable other organisations may be included.
The National Security Advisor to the Prime Minister coordinates Canada's security and intelligence community and, together with the Deputy Minister of National Defence, is responsible for the Communications Security Establishment. The National Security Advisor also oversees the provision of intelligence assessments to the Prime Minister, other ministers and senior government officials (website Privacy Council Office).
The key policy document addressing Canadian national security is "Securing an Open Society: Canada's National Security Policy" from April 2004. It defines three core national security interests:

- protecting Canada and Canadians at home and abroad,
- ensuring Canada is not a base for threats to our allies; and
- contributing to international security.

It aims to create an integrated security system to address security issues across government. The scope of the national security policy has six key strategic areas: intelligence, emergency planning and management, public health (e.g., contamination of food and water), transport security (e.g., aircraft/ airport security), border security, and international security.
CSIS is Canada's security and intelligence agency. CSIS is mandated to collect, analyze, and retain information and intelligence regarding activities that may pose a threat to the security of Canada (O'Connor 2006, p. 129). CSIS is also empowered to investigate foreign states and foreign citizens (but not Canadian citizens) more broadly in relation to the "defence of Canada" or "the conduct of the international affairs of Canada", should the Minister of National Defence or the Minister of Foreign Affairs request this assistance (see section 16 CSIS Act). Six priority areas have been identified for CSIS (O'Connor 2006, p. 130/31):

(1) terrorism;
(2) proliferation of weapons of mass destruction;
(3) espionage and foreign-influenced activities;
(4) transnational criminal activity;
(5) information security threats; and
(6) security screening and assessments.

According to CSIS, domestic terrorism "includes the threat or the use of violence by groups advocating for issues such as the environment, anti-abortion, animal rights, antiglobalization, and white supremacy, and the dissemination of militia messages by groups in the United States, and secessionist violence" (website CSIS).
An Integrated Threat Assessment Centre (ITAC) has been established within the CSIS to provide comprehensive threat assessments as a first step in the integrated security system. The threat assessments are shared within the intelligence community and law enforcement, among others (see ITAC 2007; O'Connor 206, p.131). For the preparations of a security intelligence report on someone several conditions need to be met, including (O'Connor 2006, p.137):

- The individual must be assessed as posing a significant threat to the security of Canada;
- CSIS must have sufficient threat-related information and intelligence;
- That information must be reliable and from multiple sources;
- The removal must be of strategic value in light of CSIS' investigative priorities, and
- CSIS must have sufficiently releasable open-source information to support the unclassified summary document.

Another intelligence agency is the Communications Security Establishment Canada (CSEC). This is the civilian agency of the Department of National Defence. It provides two key services: foreign signals intelligence in support of defence and foreign policy, and the protection of electronic information and communication. It is mandated to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Canadian intelligence priorities.

9.3 Practice of surveillance

In Canada, telecom service providers are not by law required to provide interception capability. Under the proposed Modernization of Investigative Techniques Act (MITA), telecommunications service providers would have been required to have intercept capable networks. The MITA would also have required telecommunications service providers to provide to designated officials,

upon request, a subscriber's contact information. This would have included a subscriber's name and address, telephone number, e-mail address, Internet Protocol address and similar basic identifiers. However, after introduction in parliament in November 2005, it died when the liberal government was defeated in December 2005 (Young 2007).

A 2006 public opinion survey suggested that 49% of Canadians are willing to exchange personal privacy safeguard for more investigative powers for government to increase security (Ekos cited by SIRC 2006, p. 16; see also Brown Goldfarb 2004). However, some recent developments suggest that Canada takes into account the effect of current law before passing new legislation. In 2004, an attempt to assess the impact of ATA for the security of Canada by a number of academic scholars in terrorism indicated that it was too early for an assessment as many of the most contentious powers under it had not been used (Gabor 2004, p.59). In 2007, the sunset clauses (clauses that expire after a given date unless extended) on investigative hearings and recognisances with conditions (preventive arrests) of the Anti-Terrorism Act 2001 (ATA) were not extended by The House of Commons.

Further, the number of wiretaps in Canada that have been warranted has been assessed by Albrecht et al. (2003) as very low in comparison with other western societies. According to Albrecht et al. (2003) Canada had in 1999 approximately 0.4 wiretaps per 100,000 citizens. The Security and Intelligence Review Committee (SIRC) reported that the Federal Court approved 176 warrant applications of CSIS in 2006-07, 227 applications in 2005-06, 247 in 2004-05 and 198 in 2003-04 (SIRC 2007, p. 53). In 2006-07, all warrant applications were approved while in 2005-2006, two applications were not (SIRC 2007, p. 53; SIRC 2006, p.48). In 2007, CSIS was required in three instances to modify the warrant application before they were approved (SIRC 2007, p.54). The statistics do not specify to what extent the warrants involved telecommunications.

The Minister of Public Safety publishes as a legal obligation (Criminal Code section 195) the number of interceptions of telecommunications by law enforcement. Also this number has dropped: from 1679 interceptions in 2002 (5.2 per 100,000 citizens) to 584 interceptions (1.8 per 100,000 citizens) in 2005 (Minister of Public Safety 2007). More recent data is not available (see table 9.1). In this period of decline there were no legislative changes that would have made obtaining a warrant any more (or less) difficult. The decline might be the result of law enforcement using other investigative methods in dealing with these offences.

Method of interception	Number of interceptions				
	2002	2003	2004	2005	2006
Telecommunication	1679	1187	1049	584	403
Microphone	179	119	100	65	46
Video	38	38	37	21	7
Other	239	154	70	67	79
Total	**2135**	**1498**	**1256**	**737**	**535**

Table 9-1 Method and number of interceptions by law enforcement 2002-2006 (Minister of Public Safety 2007)[32].

Also the most current information on telecommunication interception confirms Albrecht et al. 's (2003) findings: Canada has a relatively low number of interceptions of telecommunication.

[32] It was noted that the data reported for 2006 will likely rise in future reports as data updates are received.

9.4 Balancing national security needs with privacy

In chapter 3, we developed six principles relevant for this research. These principles are:

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.

Principle 5: guaranteed accuracy of the data for the purposes of use.

Principle 6: individual participation in the process whenever possible.

These principles stemming from a European context, reflect what the Canadian Supreme Court found in R. v. Collins: "a search will be reasonable if it is authorised by law, if the law itself is reasonable, and if the manner in which the search was carried out is reasonable" (Young 2007, p. 48). This not only applies to the quality of the law, but also to the quality of the execution of the search. In this section, we will provide for each principle an assessment of the extent to which Canada adheres to these principles.

9.4.1 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.

The right to privacy finds its basis in Canada's Charter of Rights and Freedoms, sections 7 and 8:

> Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice (section 7)
>
> Everyone has the right to be secure against unreasonable search or seizure (section 8)

Also the Privacy Act imposes obligations on federal government departments and agencies to respect privacy rights by limiting the collection, use and disclosure of personal information. CSIS investigations and CSIS investigational records (pertaining to activities suspected of constituting threats to Canada) are exempted from the Privacy Act and accompanying policies. The Personal Information Protection and Electronic Documents Act (PIPEDA) sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities.
Further, each province and territory may have specific privacy laws governing the collection, use and disclosure of personal information held by government agencies, such as for health information.

With the introduction of the Canadian Security Intelligence Act (CSIS Act, R.S.C. 1985, c. C-23), Canada was among the first countries that established a legal framework for its security service, defining the tasks, powers and control mechanisms (see Filmon 2007). The CSIS Act, Ministerial Direction, National Requirements for security intelligence, and CSIS operational policies are the legislative and policy framework of CSIS (Filmon 2007, p.39). Further, the Anti-terrorism Act 2001 (ATA) amending the CSIS Act applies. The Anti-terrorism Act strengthened the capacity of intelligence services to intercept the private communications of Canadians for certain purposes (Commission Smith 2007). Concerning telecommunications also the following legislation are relevant: Telecommunications Act, Radiocommunication Act, Radiocommunication Regulations (SOR/96-484), and Radiocommunication Act (Paragraph 9(1)c) Exemption Order (National Defence and Security).

The necessity criterion

The CSIS is mandated to address "threats to the security of Canada". This means (art. 2 CSIS Act):

(a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,
(b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,
(c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and
(d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada,

but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).

The CSIS Act authorizes the investigation of threats to the security of Canada and, the collection of information respecting activities that may, on reasonable grounds, be suspected of constituting such threats (Canadian Charter of Rights Decisions Digest 2004).
The Minister that oversees CSIS can issue "Ministerial Directions" that serve to guide CSIS operations (Section 6(2) of the CSIS Act). While the existence of the Directions is public knowledge; the content is not. The understanding of the Privacy Commissioner is that these Directions provide overarching guidance about how CSIS is expected to function, including how it is expected to balance privacy and national security interests. According to SIRC (2007), the latest direction dates from June 2007; the National Requirements for Security Intelligence for 2006–08.

Transparency in what data can be claimed

CSIS can collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada (art. 12 CSIS Act).

With a judicial warrant CSIS can intercept any communication or obtain any information, record, document or thing (section 21(3) CSIS Act). This includes any information held by a telecommunication operator on a specific individual.

However, CSIS may only request information from telecommunication service providers that those providers already collect. CSIS cannot demand providers to collect information that the providers do not already collect. In this respect, the PIPEDA for the private sector and the Federal Privacy Act for federal government provide the framework for the availability of data that may be used by CSIS.
For telecommunication data, there is not a minimum standard data set that should be stored by telecom providers. In addition, despite the Canadian Standards Association Model Code for the Protection of Personal Information, implemented in the PIPEDA (section 4.5.2/3 PIPEDA) providing that personal information shall be retained only as long as necessary for the fulfilment of the purposes for which it was collected, there is no strict standard on minimum or maximum retention periods (Warner 2005). Recent litigation in Canada has shown that providers collect different types and amounts of data and retain it for different lengths of time; there is no industry standard (see for the practise in IP-addresses: *BMG v. John Doe*; Written testimony of Shaw Communications Inc.).
The Federal Privacy Act rules (Section 6(3)) that federal government "shall dispose of personal information under the control of the institution in accordance with the regulations and in accordance with any directives or guidelines issued by the designated minister in relation to the disposal of that information."

Sensitive data
CSIS is able to collect any and all personal data in the course of an investigation, regardless of its sensitivity, provided a warrant is in place. Unlike European data protection laws, Canadian privacy law and related legislation does not specifically address the collection, use and disclosure of sensitive data. Collection, use and disclosure of this data, however, is circumscribed by constitutional protections (the Charter of Rights and Freedoms), operational policies and ministerial directions, court jurisprudence on surveillance methods, warrant conditions, and administrative oversight from both the Security Intelligence Review Committee (SIRC) and the Inspector-General of CSIS.

Transparency of the means available to intelligence agency
CSIS has a wide variety of means at its disposal. Information comes from many sources including (O'Connor 2006, p. 129 referring to Website CSIS):

- members of the public;
- foreign governments and their agencies;
- human sources;
- technical interception of telecommunications (e.g., wire-taps) and electronic surveillance of targeted persons or places (e.g., placing 'bugs');
- other government national security actors; and
- open sources, including newspapers, periodicals, academic journals, foreign and domestic broadcast, official documents and other published materials.

The CSIS Act is non-specific in these matters. The use of informants, infiltrants, or other special investigative means is not specified. Therefore, it is not without doubt whether Canada adheres to the transparency requirements of principle 1.

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

In balancing privacy and national security interests a first step is to determine whether the right to privacy is invaded; is there a reasonable expectation of privacy?

Interferences with the reasonable expectation of privacy

The use of invasive technology must be looked at in context and in relation to the nature and quality made accessible by the technology and to whom, and what information is exposed to the public (*R.v. Tessling*).

In the instance of surveillance of a car through a beeper, *R. v. Wise* considered that a beeper is a very rudimentary extension of physical surveillance attached to a car, not a person. In addition, the device was unsophisticated and inaccurate; it provided only a very rough idea of the vehicle's location. The device, for example, was unable to track the location of the vehicle at all times. Finally, the beeper merely helped the police to gather evidence which, to a great extent, was already obtained by visually observing the car (*R. v. Wise*). The Supreme Court ruled a minimum intrusion of the expectation of privacy.

Depending on the circumstances, the expectation of privacy can be higher or lower although the infringement seems to be similar at first sight. In some instances, revealing traffic data of telecommunications can be more intruding than revealing the content of the communications. For example, the daily conversation with a family member may be considered less infringing than a nonsense conversation with an assumed stranger who appears to be one's mistress. Similarly, information on a visit to a gay party can be infringing for some (those who had not yet come out of the closet) while others are not bothered by it (those that did come out of the closet a long time ago). Thus, the expectation of privacy varies by its circumstances, depending on who infringes, who's privacy is infringed upon, by what, when, how, how intense, where, and how frequent.

Principled approach: balancing through a catalogue

The privacy expectation doctrine implies that the balancing, which must be undertaken to apply for and to consent to use of privacy interfering means, will vary with the facts presented on each application. Provided the bewildering array of different techniques available to the police the approach of a judicial "catalogue" of what is or is not permitted by Section 8 of the Charter has been found scarcely feasible in *R. v. Tessling*. However, the CSIS Act provides a general catalogue. On a case-by-case basis, the exact means will be decided for and finally approved by a judge.

Balancing through a privacy impact assessment

A privacy impact assessment (PIA) may be helpful in the balancing of privacy and fundamental rights with the national security interest. The Federal Privacy Act enumerates 10 principles often referred to as the "Code of Fair Information Practices": Accountability, Collection, Consent, Use, Disclosure and Disposition, Accuracy, Safeguarding, Openness, Individual Access, and Challenging compliance (see also Marx 1998, p. 172). Since 2002, federal agencies are required to address these 10 principles through a privacy impact assessment for proposals for programs and services that raise privacy risks. Privacy issues need to be considered throughout (re-)design, implementation and evolution of federal programs or services (Lemieux 2007).

Creating a data flow table identifying how information flows or may flow through an organisation may be extremely useful in determining potential privacy risks. Further, questionnaires appended to the PIA are used to determine any significant privacy issue that need to be considered or addressed. In each questionnaire the 10 principles are addressed through several questions.

Provided that both CSES and CSIS are federal institutions, their activities are required to conform to the Charter, Privacy Act and any other applicable legislation (see Canadian Government 2007, chapter 6). However, the extent to which CSIS uses the PIA to support its applications to the Federal Court remains unknown. A PIA may be a useful instrument for any operation, including CSIS' operations, potentially interfering with the expectation of privacy.

Use of special means

Canada distinguishes warrant and non-warrant investigative techniques. For the latter the CSIS has the liberty to decide for its use. Investigations that require use of more intrusive techniques, such as the interception of telecommunications (including telecommunications data), electronic surveillance, mail opening, and covert searches are subject to a process of challenge and controls, including the use of a Federal Court warrant.[33] That is, if a CSIS official designated by the Minister believes that a warrant should be sought, he can make an application for a warrant to a federal judge.

Section 21 of the CSIS Act arranges for the warrant investigative techniques. The purpose of Section 21 is to ensure an objective, detached analysis of the facts asserted in the application for a warrant in order to determine whether the interests of the state should prevail over a person's constitutional right to be secure from unreasonable search and seizure (see Federal Court 1997; see also *Hunter* at § 32; *R. v. Thompson*).

In assessing the need for the use of a warrant investigative technique, the judge must satisfy himself that the facts establish reasonable grounds for believing that the issuance of a warrant is required (see Federal Court 1997; section 21(2)a CSIS Act). The assessment of the constitutionality of a search and seizure [..] must focus on its`reasonable' or`unreasonable' impact on the subject of the search or the seizure, and not on its rationality in furthering some valid government objective (*Hunter*).

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

The power to authorize intrusive investigation techniques rests solely with the Federal Court of Canada. Before such an authorization can be made, CSIS must provide solid justification for the proposed use of these techniques in an affidavit, which is reviewed by a CSIS committee chaired by the Director and comprised of representatives from the Department of Justice and Public Safety Canada. If the committee endorses the intrusive technique, the affidavit is submitted to the Minister of Public Safety Canada for approval. If the Minister gives approval, the affidavit is then submitted to the Federal Court, which must issue a warrant before CSIS can proceed. This judicial control function as specified in section 21 of the CSIS Act cannot be delegated to or performed by CSIS employee (see Federal Court 1997).

Criterion of subsidiary

In the application to the judge for a warrant to use special authorities, CSIS has to show that other investigative procedures have been tried and have failed or why it appears that they are unlikely to succeed (art. 21 CSIS Act)[34]. 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 (see section 21(2) CSIS Act). The application should

[33] In 1984, parliament adopted the Canadian Security Intelligence Service Act establishing CSIS. It repealed the provision of the Official Secrets Act allowing for the Solicitor General to approve wiretaps or other forms of electronic surveillance. This was replaced by a requirement that any such intrusive investigative technique be approved by a Federal Court judge (Breitkreuz 2007).
[34] This requirement does not apply (anymore) to law enforcement operations addressing terrorist offences (see Young 2007).

also include reference to any previous application made in relation to a person identified in the affidavit, including date of that application, the name of the involved judge and his decision (section 21(2) h CSIS Act).

Criterion of proportionality

The court authorization process is intended to address the balancing of national security with other interests of society by setting limits on the amount of information that can be collected, the duration of interceptions, conditions on collection, restrictions on use, among others.

The warrant shall specify the type of communication authorized to be intercepted, the type of information, records, documents or things authorized to be obtained, the identity of the person, if known, whose communication is to be intercepted or who has possession of the information to be obtained, the persons or classes of persons to whom the warrant is directed, a general description of the place where the warrant may be executed (if possible), the period for which the warrant is in force, and terms and conditions as the judge considers advisable in the public interest (Section 21(4) CSIS Act).

In the warrant, the judge may decide to have specific provisions included to enable the CSIS to investigate the threat. Examples are the "resort to" clause, and the "basket" clause. A "resort to" clause permits CSIS to intercept the communications of a target and to use the other powers granted in the warrant at a place, other than a named place, to which it believes he has resorted or will resort. The "basket" clause permits the interception of communications of unknown persons at places specified in the warrant. Warrants including these clauses have been issued (see Federal court 1997).

A clause judged to be impermissible is the "visitors" clause. This clause would permit the CSIS to use, at any place, the full range of powers granted in the warrant against the following class of persons:

(a) a person being of a specific nationality;
(b) who is admitted to Canada as a visitor;
(c) who is identified in Service data banks as a known intelligence officer, and
(d) who is a person whom the Director General of Counter Terrorism (or other person of similar level) has reasonable grounds to believe would engage in espionage (or other threat related activity) while in Canada.

The judge found that this clause unlawfully delegates the judicial control function of section 21 CSIS Act to a CSIS employee (see Federal Court 1997).

Telecommunication interception by CSES

Not always Federal Court approval is required to use intrusive investigative means. The Anti-terrorism Act (through the National Defence Act) allows the CSES to intercept private communications where one part of the communication either begins or ends in Canada as long as it is directing its activities against "foreign entities" located abroad. Unlike the CSIS, the CSES's activities involve Canadians only in those instances where, in targeting a foreign communication, it intercepts a private communication using technical means (Lamer 2005).

The CSES does not need court authorization nor is there any Charter protection afforded to foreign entities located abroad[35]. With respect to the suggestion that the CSES should be required to obtain prior judicial authorization rather than prior ministerial authorization before intercepting private communications, the former CSES Commissioner advised that executive rather than judicial authorization is necessary because warrants from Canadian courts have no jurisdiction out-

[35] The Special Senate Committee on the Subject Matter of Bill C-36 recommended in November 2001 that judicial authorization be obtained where appropriate and feasible.

side of Canada (Commission Smith 2007). This justification was accepted by the Commission Smith.

The Minister of Defence authorizes CSES interceptions based on certain conditions (Smith Commission 2007):

(a) the interception will be directed at foreign entities located outside Canada;
(b) the information to be obtained could not reasonably be obtained by other means;
(c) the expected foreign intelligence value of the information that would be derived from the interception justifies it; and
(d) satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence.

In the instance of CSES and the use of information on foreigners it seems that a different (lower) standard for privacy safeguards applies than for interferences by CSIS.

Telecommunication interception by Law enforcement

Court cases have developed a certain standard to be applied to telecommunication interception by law enforcement agencies. In the instance of state security the relevant standard might well be a different standard. This is not necessarily a lower standard (*Hunter*).

In the context of law enforcement, the Supreme Court (in *Hunter*) developed a minimum standard to be adhered to authorizing searches and seizures (through a search warrant) of section 8:

1. reasonable and probable grounds, established upon oath;
2. to believe that an offence has been committed, and
3. that there is evidence to be found at the place of the search.

Use of video surveillance requires that the judge must be satisfied by information provided under oath and in writing (i.e., a sworn affidavit) that there are reasonable grounds to believe that an offence has been or will be committed, and that information about the offence can be obtained by conducting video surveillance (Minister of Public Safety Canada 2007). These requirements also apply to other forms of surveillance, such as electronic surveillance or surveillance through telecommunications data.

R. v. Duarte (referring to *R. v. Collins*) added criteria to be considered in examining the totality of circumstances on personal data processing:

- The kind of evidence to be obtained;
- The extent to which the right of the Charter will be violated (serious or merely of technical nature);
- The urgency of the circumstances;
- The availability of other investigatory techniques;
- Will the evidence be obtained in any event;
- The seriousness of the offence;
- The extent to which the evidence is essential to substantiate the charge.

If a judge decides to approve an application for a search and seizure warrant, he may impose terms or conditions on the warrant, including conditions to ensure that the privacy of individuals is respected as much as possible during the surveillance (Minister of Public Safety Canada 2007).

Available means and required permissions

The categorisation in the CSIS Act of required consent for different activities may imply an order of privacy infringements. However, with respect to data, no order is a priori to be determined through the CSIS Act. The CSIS Act does not specify telecommunications data, and does not distinguish the content of the communication, identification data, traffic data and location data. All data applications of CSIS to telecommunication operators must adhere to the same rules and need the approval of the responsible Minister and Federal Court (see table 9.1).
However, the Courts have distinguished between the content of a message, particularly a telephone message, and the data related to the message – the length of the call, the originating number and the number called, and the location if it is a cell phone, among others. The courts have concluded the expectation of privacy is greater with respect to the content. As a result, a judge would typically require that a stronger case be made before issuing an authorization to intercept a communication.

Type of data (CSIS Act)	Examples	Decision/ Requisition by	CSIS Act article
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	Federal Court judge	21
Traffic data	Historical and future location data of cell-phone if actively been used, date and time of use	Federal Court judge	21
Content of communications	Content of an email or voice mail	Federal Court judge	21
Certain stored data (3): other data	(Historical and future) location data of cell-phone in stand-by mode	Federal Court judge	21
Data processed after requisition date and directly available to national security and intelligence	Real-time location data of cell-phone if actively been used	Federal Court judge	21
Sensitive data (1)	Data concerning racial or ethnic origin, religious or philosophical beliefs, or concerning health or sex life	Federal Court judge	21
Sensitive data (2)	Data concerning political opinions, trade-union membership	Federal Court judge	21

Table 9-2 Required approval of data according to CSIS Act

For how long can location information of mobile devices be tracked and traced?

A warrant shall not exceed sixty days for enabling CSIS to investigate a threat to the security of Canada by activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada. For other threats to the security of Canada the warrant cannot exceed one year (section 21(5) CSIS Act). Renewal of a warrant requires again a judge to balance the state's interest with the individual's (section 21(6) CSIS Act).
However, there is no requirement for (telecommunication) service providers to require automatic data retention of all subscribers or to collect or maintain accurate subscribers information (Young 2007, p.62).

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

Review of CSIS
The CSIS is reviewed by a Inspector General of the CSIS (IG), and the Security Intelligence Review Committee (SIRC). The IG has three functions (art. 30 CSIS Act):

1. to monitor the compliance by the CSIS with its operational policies;
2. to review the operational activities of the CSIS, and
3. to submit certificates to the responsible Minister stating the extent to which the IG is satisfied with the yearly CSIS report addressing CSIS operational activities. In his review the IG addresses exercises of the CSIS that in the opinion of the IG are unauthorized, or unreasonable or unnecessary.

The IG is entitled to access any CSIS information relating to the performance of the duties and functions of the CSIS as the IG deems necessary. Only exception is Confidences of Cabinet. In its certificates of 2004, 2005 and 2006, the IG has reported positively on the CSIS: CSIS has not acted beyond the framework of its statutory authority, has not contravened any Ministerial Directions, and has not exercised its powers unreasonably or unnecessarily. The IG cannot render legally binding decisions.

The SIRC is the external review committee that reports directly to Canadian parliament (Filmon 2007). It examines past operations of CSIS and investigates complaints. Its powers are limited to the activities of CSIS. SIRC also reviews CSIS use of Federal Court warrants, including warrant applications and implementation. Further, it collects warrant statistics (O'Connor 2006, p. 273).
SIRC consists of members from the Queen's Privy Council for Canada, a Council to aid and advise in the Government of Canada. Its members consists of members of the present ministry but also former ministers and other distinguished persons. Members of the review committee may, however, not be a member of the Senate or the House of Commons (Art. 34 CSIS Act). SIRC is supported by an executive director and 19 staff members (SIRC 2006). It is fully independent in what it chooses to examine and how it goes about its work (Filmon 2007).
The SIRC reviews generally the performance by the CSIS of its duties and functions, for example through reviewing the reports of the Director and certificates of the IG, but also through the compilation and analyses of statistics on the operational activities of the CSIS (art. 38 CSIS Act). Further, the SIRC may conduct or direct the CSIS, or the IG to conduct reviews to ensure adherence of the CSIS activities to the CSIS Act, regulations and ministerial directions, and that activities do not involve any unreasonable or unnecessary exercise by the CSIS of any of its powers (O'Connor 2006, p. 267). It may further investigate the CSIS to address complaints on the activities of the CSIS, among others (art. 38 CSIS Act). Also the SIRC may access any information of

the CSIS and the IG (art. 39 CSIS Act). Only exception is Confidences of Cabinet. The SIRC reports every year to the Minister and the Minister provides this report to each House of parliament (see website SIRC). SIRC cannot render legally binding decisions.

CSIS also remains accountable for its operations through the existing structure of government, specifically the Minister of Public Safety, central agencies, the Auditor General, the Information Commissioner, and the Privacy Commissioner of Canada (SIRC 2006; O'Connor 2006, p. 284).
Finally, CSIS provides information to parliament and the public through the Minister's Annual Statement on National Security and the CSIS Public Report.
Also CSIS reviews its operations. In 2005, a rejection of a warrant application by the Federal Court resulted in a moratorium of a year (June 2005- June 2006) imposed by the CSIS Director (see SIRC 2007, p.54). The moratorium was internal to CSIS and reflected its decision to stop filing warrant applications with the Federal Court (except in urgent cases), until CSIS has reviewed and improved its own processes, to prevent a reoccurrence of what triggered the initial moratorium (see SIRC 2006, p. 47-49). Thirty-eight so-called 'exceptional' warrants were considered and/or approved by a Federal Court judge.
Further, a Federal Court judge scrutinizes the legality of the measure and confirms satisfaction of the legal requirements.
Canada has a judicial control before the measure and a follow-up control mechanism through the SIRC and the IG. This is important because the judge authorizing the special investigative measure may never see how it was implemented (Cameron 2007).

Review of CSES
Review of the CSES is much more limited. The Commissioner of the Communications Security Establishment (CSE) oversees the activities of CSES (website CSEC). The Standing Committee on Public Safety and National Security (Breitkreuz et al. 2007) recommended (recommendation 44 and 45) to require the Commissioner of the CSES to review the private communication interception activities carried out under ministerial authorization to ensure they comply with the requirements of the Canadian Charter of Rights and Freedoms and the Privacy Act. It further recommends (recommendation 45) to require the CSES to only undertake activities consistent with the *Canadian Charter of Rights and Freedoms* and the Privacy Act, in addition to the restraints on the exercise of its mandate already set out in that section (website Ministry of Justice). Government replied that CSES already considers the legislative requirements for their operations, including the requirements of the Charter and the Privacy Act, and sees no reason to make this more explicit in law (Canadian Government 2007).
The CSES commissioner has argued in favour of non binding decisions by review commissions (Lamer 2005).

The Commission Smith (2007) found the SIRC and the CSES Commissioner generally to be effective oversight mechanisms. Oversight by the Commission for Public Complaints on the national security functions of the Royal Canadian Mounted Police (RCMP) are considered insufficient due to its limited powers (passive oversight only after complaints, limited access to information, no involvement in any form of continuing review of the operations of the RCMP or the adequacy of its practices).

Ubiquitous oversight of the security system
The oversight of the Canadian national security system is organised by organisation. SIRC does not have jurisdiction over the entire secret national security scene (Cameron 2007). Oversight on and review of data sharing and distribution across different organisations involved in secret national security operations may be lacking or insufficient.

At the end of 2005, the proposed National Security Committee of parliamentarians Act (Bill C-81) introduced such ubiquitous parliamentarian review on the national security community. The Bill proceeded no further due to dissolution of parliament. It would have included members from parliament (both Senate and House of Commons) including the opposition. The mandate provided to the proposed committee appeared to be broad enough to allow it to engage in on-going compliance audits of the departments and agencies making up the security and intelligence community in Canada (Breitkreuz et al. 2007, p. 84-85). The Standing Committee on Public Safety and National Security recommended to introduce such a ubiquitous parliamentary oversight as soon as possible (Breitkreuz et al. 2007; see also Commission Smith 2007).
The Government response warns for the danger of overlapping reviews and duplication of efforts, and broad and unfocused proceedings if ATA would be the basis for the parliamentary oversight. It stresses the importance of the thematic nature of the subject matter and the issues that arise from time to time. It is considering options for an enhanced role for parliamentarians as a key part of an improved national security review framework (Canadian Government 2007, chapter 10).

Complaints
Complaints on CSIS should first be submitted to the Director of the CSIS. If the response of the Director is not received in time or is dissatisfactory to the complainant, the complaint may be made to the SIRC. Anyone can file a complaint to the SIRC concerning any act or thing done by the CSIS (art. 41 CSIS Act). If the SIRC judges the complaint as appropriate (e.g., not trivial or made in bad faith), it will investigate the complaint (art. 41 CSIS Act). In its investigation the CSIS, and the complainant will be provided the opportunity to make representations to the SIRC. The SIRC may ask the Canadian Human Rights Commission for advise on the complaint (art. 49 CSIS Act).
Concerning the complaint issue, the Standing Committee on Public Safety and National Security (Breitkreuz et al. 2007, p. 78) identified possible improvements in the private pre-hearing conferences of a complaint, which private nature of CSIS witnesses currently put the complainant at a disadvantage.
SIRC has received in 2005 46 complaints, 2006 63 complaints, and in 2007 61 complaints (SIRC 2007). It has issued 125 written complaint reports over the past 20 years (SIRC 2006). The SIRC reports its findings with recommendations to the Minister.

9.4.5 Principle 5: guaranteed accuracy of the data for the purposes of use.

The CSIS Act does not specify specific requirements concerning the guaranteed accuracy for the purposes of use of the data. This requirement may be taken into account by the judicial control (see section 21 CSIS Act).
Article 6(2) of the Federal Privacy Act rules that "A government institution shall take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible."

9.4.6 Principle 6: individual participation in the process whenever possible.

Except for complaints on activities of CSIS, individuals are withheld from participation in the process. Individuals will not be informed of their communications being intercepted, even if this would not harm any CSIS operations. The Federal Privacy Act addresses this issue in article 22 (1) a. Government may refuse to disclose any personal data if these were collected for investigations pertaining to activities suspected of constituting threats to the security of Canada within the

meaning of the CSIS Act, among others. This information can be withhold as long as the information came into existence less than twenty years prior to the request.
Only in the instance of security clearance, the CSIS Act requests to inform the individual of the denial of the security clearance (art. 42 CSIS Act).

Canada generally adheres to the principles developed. Although it may be questioned whether Canada fulfils the transparency requirement for the available means to address national security threats, the balancing process can be summarised as adequate.

9.5 Developments Canada

Also in Canada developments have stressed the balance between privacy and security interests of society towards the latter. For law enforcement, the ATA has eliminated the need to demonstrate that electronic surveillance is a last resort in the investigation of terrorist offences, which is an exception to the general rule applicable in other circumstances. It further extends the period of validity of a wiretap authorization from sixty days to up to one year when police are investigating a terrorist offence; and permits a delay of up to three years in notifying a target after surveillance has taken place, as opposed to the 90 day period that is applicable for other criminal offences (see Young 2007).
Despite these developments, other developments were not approved, such as the MITA and the extension of the sunset clauses in the ATA.

9.6 Summary on Canada

Privacy in Canada
Canada is generally considered to have a high level of privacy safeguards. Its understanding of privacy is captured by the reasonable expectation of privacy doctrine. The doctrine is based on what privacy people reasonably can expect in a free and democratic society. The degree of protection depends on the reasonable protection of privacy of the individual in the circumstances. Generally, the interception of telecommunications, including location data, is considered to interfere with the reasonable expectation of privacy.
Federal agencies are required to address privacy through a privacy impact assessment for proposals for programs and services that raise privacy risks. Privacy issues need to be considered throughout (re-)design, implementation and evolution of federal programs or services.

Interferences with the reasonable expectation of privacy
Federal Court warrants are required for intrusive investigative means such as telecommunication data requests. Before applying for a warrant, Canada Security and Intelligence Service (CSIS) balances the national security interest with other interests, including the privacy interest of individuals. The Security and Intelligence Review Committee (SIRC) may review the execution of the warrant by CSIS, and rule on complaints of activities of CSIS.
Facts on the use of special means, such as the number of warrants approved and denied by a Federal Court judge are published by the SIRC. In addition, as a legal obligation, the number of interceptions by law enforcement are published. This contributes to the transparency of the use and effectiveness of government operations. There is at least some indication of the size and frequency of the use of special means. Significant increases or diminished use of special means may

readily be accessed and used by members of parliament. Uncertainty on the number of special means, gives raise to speculation and possibly unfair frightening prospective.

Number of interferences relatively low

Interferences with the reasonable expectation of (Location) privacy is also limited due to several other aspects. Telecommunication service providers are not by law required to provide interception capability. Further, there is no requirement for (telecommunication) service providers to require automatic data retention of all subscribers or to collect or maintain accurate subscribers information. Moreover, strict general requirements on data retention for telecommunication operators (e.g., with respect to type of data, length of time to store) is non-existent.

These aspects guarantee that the use of the cell-phone data is primarily for the purposes for which it is collected. In this respect, national security and law enforcement are not the core focus of data retention in telecommunication. The length of time telecommunication data will be stored, depends on the purpose of the processing, to enable the communications and to bill the user. As soon as the communication has ended and the bill has been paid, the data will typically be removed. The data retention varies among providers, but is typically far less than the European requirement of a minimum of six months. This may explain why Canada has, according to the published public figures, compared to the other cases in this report, a small number of telecommunication taps and/or warrants both in absolute and relative terms.

Also the non-specific telecommunication data clause in Section 21 of the CSIS Act serves the privacy of Canadians relatively well. CSIS can only obtain any telecommunication data through a Federal Court order; in the CSIS Act, no difference is made between identification data, traffic data, location data, the timeliness of the data (real-time v. historical data), and the use of the cell-phone (either active or non-active (standby)). Also sensitive data such as data on one's religion or race is not specifically addressed in Canadian privacy law and related legislation. The Courts are expected to balance each application respecting the 'totality of the circumstances'. The totality may vary per case, and the introduction of a catalogue of (presumably) standard applications that automatically would obtain approval from the Court, was considered scarcely feasible by the Federal Court.

Finally, although adherence to the transparency requirements of principle 1 may be doubted, some support may be found for the suggestion that the greater the transparency of which means can be used for certain categories of crime, the more they will be used. Or in the instance of Canada, the lack of transparency may have resulted in a relatively low number of wiretaps. This may also be explained by the use of other more appropriate means, the lack of legislation requiring a interception capability on the telecommunications networks, or because of the balance between national security or law enforcement with privacy was favouring the latter.

Role of location technology

The role of location technology and information compared to other techniques remains unresolved. The use of these means are not transparently provided in the law or otherwise specified other than any means. Nor did this research find documents of parliament discussing or specifying the means available to CSIS for specific circumstances or cases.

No ubiquitous oversight for security sector

Canada has several organisation that have a security task. Each of these organisations have some kind of review mechanism in place. However, As Cameron (2007) explained these organisation specific safeguards with respect to review may imply gaps or overlap in reviews of both domestic and international cross organisational data and intelligence use/ exchange. It is recommended to review the current situation and to identify gaps or overlaps. Ultimately, a new review body may be necessary to provide a safeguard that meets the Canadian privacy standard.

10 Germany: balancing privacy and national security

This chapter focuses on the way privacy and national security interests are balanced with respect to the use of location information of mobile devices for national security purposes. First, it addresses how privacy as a general concept is considered in Germany. In the second section, German national security is addressed and some practical information on surveillance provided. In section 3, the balancing of national security needs with privacy is assessed through the balancing principles developed in chapter 3. Finally, conclusions are presented in section 4.

In 2007, Germany has approximately 82 million people spread over an area of 357,021 sq km (worldfactbook 2008). Germany is a member of United Nations, OECD, the Council of Europe, and the European Union.

10.1 Privacy in Germany

Privacy International & EPIC has qualified Germany's privacy law as one of the strictest in Europe (Rotenberg et al. 2006). Germany was assessed to have significant privacy protections and safeguards for almost every researched aspect (including constitutional protection, statutory protection, privacy enforcement, communications interception, data sharing, visual surveillance, and communication's data retention).
In 2007s Privacy international and EPIC's survey, Germany's privacy qualification dropped significantly to a "some safeguards but weakened protections" partly due to the implementation of the Data Retention Directive. Protections towards surveillance of medical, financial and movement were still assessed to be significant (Privacy International et al. 2007).

10.1.1 Right to privacy

There is no general right to privacy in the German Basic Law (*Grundgesetz*). Instead, it is linked to the concept of human dignity and personality. The legal basis for the principle right to privacy is in the German Basic Law articles 1 (dignity) and 2 (personality). Human dignity is absolute (*unantastbar*). It must be respected and protected.[36] Article 2 of the Basic Law guarantees that "[e]very person has the right to free development of his personality, insofar as he does not injure the rights of oth-

[36] German Basic Law (*Grundgesetz*) reads:

Art 1

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

(2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.

(3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

Art 2

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

ers" (translation by Whitman 2004). It protects the right to act as one pleases and ensures that one can freely develop his personality without having to consider the expectations of society (Jacoby 2006, p.22; Whitman 2004). Thus, the protection of privacy in the German tradition can be regarded as an aspect of the protection of one's 'personality'. Whitman (2004) argues that this implies the ability to exercise free will, and the defining characteristic of creatures with free will was that they were unpredictably individual. Each individual should be able to fully realize his potential as an individual: to give full expression to his peculiar capacities and powers.

In the *Census Act Case* (*Volkszählung* 1983) the Federal Constitutional Court stated that under Articles 1 and 2 of the *Grundgesetz* an individual has "the authority to decide for himself, on the basis of the idea of self-determination, when and within what limits facts about his personal life shall be disclosed" (Jacoby 2005, p.1090). The Court noted that if a person is unable to oversee what of his personal information is available in specific contexts, it could impact his decisional freedom (Jacoby 2006, p.33). Technological developments provided, the Court was concerned about the possibility that government officials could use automatic data processing to construct a 'complete personality profile' (Jacoby 2005, p.1090). In 2005, in addressing the permissibility of GPS surveillance, the Court reaffirms that the degree of privacy protection depends on the nature of the information, which the technology discloses. When the GPS data are combined with other surveillance techniques in ways that yield too comprehensively the construction of a personality profile (*umfassenden Persönlichkeitsprofils*), the use of a tracking device may violate a suspects' constitutional right to 'Informational self-determination' (Ross 2005, p.1810).
Although the Court determined that the use of GPS as a surveillance tool did not violate Articles 1 and 2 of the Basic Law, the Court also made clear that other emerging surveillance technologies could be constitutionally impermissible (Jacoby 2005, p.1092). The Court also stated that the right to informational self-determination was not unlimited and that certain restrictions on an individual's right to informational self-determination for reasons of compelling public interest would be acceptable (Jacoby 2005, p.1091).

10.1.2 Specific aspects of privacy in legislation

Article 10 and 13 of the Basic Law address specific rights to privacy. Article 10 concerns the privacy of post and telecommunications and article 13 the privacy of the home.

Article 13: inviolability of the home
Under German law, the right to privacy must especially be respected in homes. In the *Lauschangriff Case* (2004), the Court ruled that acoustic surveillance of the home by the state was constitutionally prohibited. The home was considered the most private place where all citizens were entitled to a sphere of intimacy in which to conduct private conversations without fear of government intrusion: the 'last refuge' for the development of one's personality and preservation of one's dignity. One may choose to forego writing letters or making telephone calls to preserve their privacy, but the right to retreat into one's home is absolute (Jacoby 2005, p.1090). Therefore, people enjoy less protection for privacy in public areas than in their home or workplace. Filming a suspect in public is permissible, while filming him in his home is not. But appearing in public only diminishes privacy protections; it does not cancel them altogether. Surveillance can only be conducted with judicial authorization even if the surveillance is completely in public areas (Ross 2005, p.1810).

Article 10: inviolability of post and telecommunications

Article 10 of the Grundgesetz (Basic Law) protects the post and telecommunication from government intrusions, among others. It reads (translation ECtHR in *Weber*):

> 1. Secrecy of mail, post and telecommunications shall be inviolable.
> 2. Restrictions may be ordered only pursuant to a statute. Where such restrictions are intended to protect the free democratic constitutional order or the existence or security of the Federation or of a *Land*, the statute may provide that the person concerned shall not be notified of the restriction and that review by the courts shall be replaced by a system of scrutiny by agencies and auxiliary agencies appointed by the people's elected representatives.

The inviolability of telecommunications privacy seeks to avoid that the exchange of opinions and information by means of telecommunications equipment ceases altogether or is modified in its form and content. This is because communication partners do not expect government to interfere with their communication, or to take note of the circumstances or the content of their communication (Federal Constitutional Court 1999 at 162).

The protection of fundamental rights (i.c. telecommunications) is not only restricted to shielding the content of the communication. The Federal Constitutional Court has ruled that the protection of fundamental rights also covers the circumstances of communication, particularly including: (1) information about whether, when and how often telecommunications traffic has taken place or has been attempted; (2) information about the individuals between whom telecommunications traffic has taken place or has been attempted; and (3) information about which subscriber lines have been used. The state cannot claim to be allowed to take note of the circumstances of acts of communication. The use of the medium of communication is supposed to remain confidential in all respects (Federal Constitutional Court 1999 at 161).

Article 10.2 of the Basic Law permits restrictions of telecommunications privacy. The Federal Constitutional Court (1999 at 219) ruled that because individuals are integrated in the community and depend on the community, they must tolerate restrictions of their fundamental rights if they are justified by prevailing public interests. Such restrictions require a legal regulation that serves a legitimate aim in the public interest and respects the principle of proportionality (Federal Constitutional Court 1999 at 164).

Thus, privacy in Germany can be considered as the right to self-determination, a limited access to self including limited access to one's personal data. In addition, telecommunications, both the content and the circumstances (e.g., traffic and location data), are protected by the German constitution. Restrictions of privacy are permitted if these are justified by prevailing public interests.

10.2 Protecting National security in Germany

For several decades, Germany has experienced threats to its national security (e.g., *Rote Armee Fraktion* (RAF), PKK). At the federal level there are three security and intelligence agencies operating: the *Bundesamt für Verfassungsschutz* (BfV, "Federal Office for the Protection of the Constitution"), the *Bundesnachrichtendienst* (Federal Intelli-

gence Service, BND) and the *Militärischer Abschirmdienst* (military security and intelligence service, MAD). Here, we focus on the BfV. Where applicable reference is made to the BND.

The Bundesamt für Verfassungsschutz

The BfV is Germany's domestic intelligence agency. Its main function is the surveillance of anti-constitutional activities in Germany. Its' 16 counterparts at the Land level are the Landesämter für Verfassungsschutz (LfVs; State Offices for the Protection of the Constitution).

BfV and the LfVs are tasked with the collection and analysis of information, especially of such information, intelligence and documents relating to individuals or subject-matters, concerning

1. 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;
2. activities threatening security or intelligence activities carried out on behalf of a foreign power within the area where this Act applies;
3. efforts within the area where this Act applies, which jeopardise foreign concerns of the Federal Republic of Germany by the use of violence or preparation thereof;
4. efforts within the area where this Act applies, directed against the idea of international understanding (Art. 9 §2 of the Basic Law refers), especially against the peaceful coexistence of peoples (Art. 26 §1 of the Basic Law refers).

(§ 3(1) BVerfSchG; website BfV).

Focus of the BfV is currently on (website BfV):

- (German) right-wing extremism/- terrorism;
- (German) lef-wing extremism/ - terrorism;
- extremism of foreigners;
- Islamism (extremism/ terrorism);
- Espionage, security and countersabotage;
- Scientology.

The federal law pertaining to the BfV is the "Act Regulating the Cooperation between the Federation and the Federal States in matters relating to the Protection of the Constitution and the Federal Office for the Protection of the Constitution" - *Bundesverfassungsschutzgesetz* (BverfSchG). BfV employs approximately 2400 people (O'Connor 2006, p.339).

Every state also has its own Office for the Protection of the Constitution, with a structure comparable to that of the BfV. Each office has regional jurisdiction and is subject to state regulation. The BfV does not have direct control over the activities of the state offices, but is required to co-operate with them. When a surveillance target's activities extend beyond the territory of a single state, the BfV will take over responsibility for the investigation. Intelligence gathered by the states is stored centrally by the BfV (O'Connor 2006, p. 339).

Bundesnachrichtendienst

The *Bundesnachrichtendienst* (BND) is the foreign intelligence agency of the German government, under the control of the Chancellor's Office.

The BND acts as an early warning system to alert the German government to threats to German interests from overseas. It depends heavily on wiretapping and electronic surveillance of international communications. It collects and evaluates information on a variety of areas such as international terrorism, WMD proliferation and illegal transfer of technology, organized crime, weapons and drug trafficking, money laundering, illegal migration and information warfare. BND may not target the individual communications of German citizens. BND has approximately 6000 staff members (O'Connor 2006, p.340).

The MAD focuses on anti-constitutional activities within the German armed forces and on activities against the German armed forces such as espionage. The MAD employs approximately 1300 people (O'Connor 2006, p. 340).

G 10 Commission
The independent G 10 Commission decides on the necessity and admissibility of restrictions on the privacy of correspondence, posts and telecommunications pursuant to Article 10 of the Basic Law as well as on specific data categories as specified in § 8 of the BVerfSchG.
The G 10 Commission consists of a president who is qualified to hold judicial office and three additional members who are appointed by the parliamentary Supervisory Board for the duration of one legislative term and who are independent in the exercise of their functions (§ 15(1) G 10 Act).

10.3 Practice of surveillance

Albrecht et al. (2003, p.6) have assessed that Germany has approximately 15 wiretaps on telecommunication per 100,000 citizens. This was a moderate percentage compared to other countries. The number of wiretaps has increased significantly from 3,828 wiretaps in 1997 to 18,110 taps in 2001 (Albrecht et al. 2003, p.9). However, Albrecht et al. (2003, p. 8) notice that the relative percentage on wiretapped cell-phones decreased from 0.5 cell-phones per 1,000 cell phones to 0.3 cell-phones per 1,000. Thus, the number of cell-phones is growing faster than the number of wiretaps. The number of taps on cell-phones has increased from 6,391 in 1998, to 29,017 in 2004 and 35,816 in 2006 (Bundesnetzagentur 2007, p. 119; Heise online, 2005 & 2007). Since 2002, the absolute increase was approximately 5,000 taps per year. In 2006, the increase in the number of new taps has dropped to a thousand taps. This suggests that a new 'balance' has been found. The number of taps on permanent phones has remained relatively constant around 5,000 taps.
The number of taps on cell-phones may be explained by the growing number of cell-phone users and the number of cell-phones one may have (e.g., one for work, one for private use for each member of the family).

Albrecht et al. (2003) assessed that almost in 75% of the convictions at least one wiretap was used. However, the data from the wiretap was only of limited significance for the evidence of the case (Albrecht et al. 2003, p.28). Zöller (2004) noticed that 66.5% of the convicted persons concerned minor crimes (less than five years of detention).

10.4 Balancing national security needs with privacy

In chapter 3, we developed six principles to which personal data processing should adhere to. These principles are:

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.

Principle 5: guaranteed accuracy of the data for the purposes of use.

Principle 6: individual participation in the process whenever possible.

In this section, we will provide for each principle an assessment of the extent to which Germany adheres to these principles.

10.4.1 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.

A wide variety of German legislation applies to the surveillance and privacy aspects. Particularly the following legislation is relevant:

- Basic Law of Germany (*Grundgesetz für die Bundesrepublik Deutschland*)
- G-10 Act (Act on Restrictions on the Secrecy of Mail, Post and Telecommunications) (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10)*
- Act Regulating the Cooperation between the Federation and the Federal States in Matters Relating to the Protection of the Constitution and on the Federal Office for the Protection of the Constitution *(Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz* (Bundesverfassungsschutzgesetz - BVerfSchG))
- BND-Act, Act on the Federal Intelligence Service (*Gesetz über den Bundesnachrichtendienst (BND-Gesetz - BNDG)*)
- Telecommunication act – *(Telekommunikationsgesetz (TKG))*
- Ordinance concerning the Technical and Organisational Implementation of Measures for the Interception of Telecommunications (Telecommunications Interception Ordinance - TKÜV)- *(Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (TelekommunikationsÜberwachungsverordnung- TKÜV)).*

- Telecommunications Customer Protection Ordinance (*Telekommunikation-skundenschutzverordnung (TKV)*)
- Counter-Terrorism Act II replacing the Counter-Terrorism Act – (*Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes* (TBEG) vom 5. Januar 2007; Terrorismusbekämpfungsergänzungsgesetz (TBEG); (). (BGBI 1 seite 2))
- Data protection act – *(Bundesdatenschutzgesetz (BDSG))*
- Act implementing EU Data retention directive 2006/24/EC – (*Gesetz zur Neuregelung der Telekommunikations¨uberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG*)

The legislative framework provides indications when one may expect an interference with the right to privacy. The instances for individual monitoring and strategic monitoring are discussed below.

Individual monitoring
BfV is tasked with individual monitoring, the interception of telecommunications of specific persons. It serves to avert or investigate certain grave offences which the persons monitored are suspected of planning or having committed (*Weber*).
Personal data (*personenbezogene Daten*) obtained through the interception of telecommunications can only be processed if the person concerned is either subject to individual monitoring because of mere factual indications (*tatsächliche Anhaltspunkte*) for planning, committing, or having committed one of the offences listed in the G-10-Act and in certain other provisions, such as the Criminal Code. These offences include high treason against the peace or security of the State, crimes threatening the democratic order, the external security of the State or the security of the allied forces based in Germany, the formation of terrorist associations, murder, manslaughter, robbery, infiltration of foreigners and the production, importation and trafficking of illegal drugs, participation in organisations that aim to commit criminal facts directed at the democratic order, or the security of the state or one of its *Länder* (G-10 Act § 3(1); *Weber*). For high treason against the peace or security of the State (as specified in BVerfSchG §3(1).1, the special data authority can only be used if inciting hate or arbitrary rule against parts of the society is involved, or if it involves the use or preparation of violence including the support of organisations that support such efforts (BVerfSchG § 8a(2)).

Strategic monitoring of international telecommunication
BND is tasked with strategic monitoring. This aims at collecting information by intercepting telecommunications in order to identify and avert serious dangers facing Germany. § 5(1) of the G-10-Act provides that restrictions on the secrecy of telecommunications are permitted only to collect information about which knowledge is necessary for the timely identification and avoidance of certain dangers. These are:

1. an armed attack on the Federal Republic of Germany;
2. the commission of international terrorist attacks in the Federal Republic of Germany;
3. international arms trafficking within the meaning of the Control of Weapons of War Act and prohibited external trade in goods, data-processing programmes and technologies in cases of considerable importance;
4. the illegal importation of drugs in substantial quantities into the territory of the Federal Republic of Germany;
5. threatening the monetary stability in the Eurozone through counterfeiting of money (Geldfälschung) committed abroad;

6. the laundering of money in international context in instances of significant importance.

Transparency in what data can be claimed

Restrictions in the secrecy of mail, post and telecommunications are specified in the BverfSchG and the G-10 Act, among others. The G-10 Act specifies that to protect the 'national security' telecommunications may be strategically or on an individual basis be monitored (§ 3(1)).

Monitoring by the Bundesverfassungsamt (BfV)

The BVerfSchG (§ 8(1)) rules that the BfV may claim personal data and use these in so far this does not conflict with the applicable provisions in the Federal Data Protection Act (*Bundesdatenschutzgesetz*) or other special arrangements provided for in the BVerfSchG.

Since 2002[37], the BVerfSchG (§ 8a(2, nos 1-5)) arranges for special intelligences requests by BfV. Five categories of special data can be requested:

1) data from airline companies (data on names, addresses and the use of transport services and other circumstances of air services);
2) data from credit institutions, financial service institutes and financial institutions (data on accounts, account holders and other entitled parties as well as other individuals involved in payment transactions and on monetary transactions and investments);
3) data from individuals and companies providing postal services on a commercial basis (data on names, addresses, post office boxes and other circumstances of postal services);
4) traffic data from companies providing telecommunications services and
5) traffic data from commercial teleservices.

With respect to traffic data, the law refers to the Telecommunication law (§ 96 § 1 – 4) and other data that are required for the set-up and maintaining of the necessary traffic data. The teleservice providers are required to provide data that identify the user of a service, data concerning the beginning, ending, and volume of the service being used, and data concerning the used service (for example, type). Data on telecommunications connections and the use of teleservices comprise:

1) identification codes, card codes, location codes and call numbers or code numbers of the terminal connections calling or being called or of the terminal equipment;
2) commencement and termination of the connection with date and time;
3) information on the kind of telecommunications and teleservices the client is making use of;
4) terminals of dedicated connections, their commencement and termination with date and time.

(English translation of BverfSchG d.d. 21 June 2005).

According to §96 Telecommunication act, traffic data include location data of the BTS that was used (information on the "Funkzelle" from which a call was initiated as well as information on the "Funkzelle" in which the call was received). Telecommunication providers assign in case of mobile devices information to each call which identifies the locality in which the call was initiated. In addition, information on the

[37] Counter-Terrorism Act replaced in 2007 by the Counter-Terrorism Act II.

location of the mobile device is generated as long as the device is operational. This type of location data is not more detailled as it refers also to "Funkzellen" (but is independent from actual communication). Passive (standby) location data of a cell-phone may be used to develop and maintain the necessary traffic data. However, the data retention law that went into force November 2007 does not require retention of such location data.
For cell-phones in the standby mode, only the real-time location data can be requested from the telecom providers (based on § 8a(2) No. 4 BVerfSchG). This may also be through silent SMSs (Bundestag 2005, 15/4725 at 55). Government uses real-time information to use the IMSI catcher to determine the location of the cell-phone more accurately. Location data (up to 6 months) can only be requested if the cell-phone was actively been used.

Sensitive data
The German data protection act (BDSG § 3(9)) has defined sensitive personal data (*besondere Arten personenbezogener Daten*) as data concerning racial or ethnic origin, religious or philosophical beliefs, political opinions, trade-union membership or concerning health or sex life. The use of these data is restricted (BDSG § 13(2)), but this restriction does not apply to the BfV for purposes of national security (see BVerfSchG § 27). The BfV can claim sensitive personal data through § 8 (1) BVerfSchG (Befugnisnorm zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten).

Monitoring by the BND
The BND is allowed to accomplish individual or strategic monitoring of telecommunications. It is only authorised to carry out international monitoring measures with the aid of catchwords (*Suchbegriffe*)[38] which served, and were suitable for, the investigation of the dangers described in the monitoring order (G-10 Act § 5(2)). That provision prohibits the catchwords from containing distinguishing features (*Identifizierungsmerkmale*) allowing the interception of specific telecommunications. However, this rule does not apply to telephone connections situated abroad if it can be ruled out that connections concerning Germans or German companies are deliberately being monitored. The catchwords have to be listed in the monitoring order (BVL building on *Weber 32*). For the identification of threats in the field of weapons proliferation, approximately 2,000 search concepts had been employed, in the field of conventional arms trade almost 1,000, in the field of terrorism about 500 and in the field of drug trade about 400. Due to the poor results in the fields of terrorism and the drug trade, these restriction orders were not renewed in 1998 (Federal Court 1999 § 87).

Transparency of the means available to intelligence agency
The security and intelligence service (BfV) may use methods, materials and instruments such as trusted persons and informants, surveillance, image and sound recordings, cover documents and cover licence plates for the clandestine collection of information which are to be specified in a service regulation at the same time regulating the responsibility for ordering such collection of information (BVerfSchG § 8(2)).

To track or localize a cell-phone, law enforcement can use data from an active/ communicating cell-phone, silent SMSs, and an IMSI-catcher to determine the location of a cell-phone. Also the Bundesamt für Verfassungsschutz (BfV) and the

[38] For example, through scanning the communication for these catch words

Bundesnachrichtendienst (BND) can use these means (Bundestag 2005, p.23). Standby data cannot be ordered so that the creation of a behaviour pattern (*Bewegungsprofile*) is impossible (Bundestag 2005, p.22).
The *Bundeskriminalamt* (BKA – Federal Bureau of Criminal Investigation) claimed only to use GPS in six to ten investigations annually, and reports suggest that police have begun to favor the tracing of cell phones (e.g., silent text messages) as a means to track the physical movements of criminal suspects (Jacoby 2005, p.1092).

The law is accessible to citizens. The tasks of security and intelligence agencies are specified by law and it is foreseeable when an interference with the right to privacy may be expected. The means available to security and intelligence agencies are transparent as are the data that may be claimed and used to protect the national security. Principle 1 is being adhered to.

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

In balancing interests of society and the interests of individuals, the important questions with respect to the fundamental rights of the individual are (Federal Constitutional Court 1999):

1. under what circumstances are how many and which holders of fundamental rights subject to impairments; and
2. what is the degree of intensity of these impairments? The standards for determining this include:
    a. which thresholds for intervention have been created;
    b. the number of persons affected; and
    c. the intensity of the impairments. The intensity of the impairment, in turn, depends on:
    (1) whether the communication partners' identities remain anonymous;
    (2) which calls and
    (3) which contents can be screened, and
    (4) what disadvantages threaten, or are justly feared by, the holders of fundamental rights on account of the monitoring measures.

On the other hand are the considerations of public interests. The decisive factors in this context are:

1. how great are the dangers that are to be recognised with the help of telecommunications monitoring; and
2. how probable is their occurrence.

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

Criterion of subsidiary
From among several appropriate measures, the BfV shall select the one prospectively least restrictive for the data subject (§9 BVerfSchG). Data from publicly accessible sources (like newspapers, flyers, programs, appeals, public events (see website BfV) or government sources (e.g., police) are considered less infringing than other means of data collection (§ 9(1) and § 18(3) BVerfSchG).

Concerning location data of terminal devices, if an interest of the BfV can be satisfied through identifying information, there is no need to claim traffic data or location data. Similarly, if traffic data can satisfy the requirements, there is no need to process the location data. If historical location data can satisfy the needs then real-time location data should not be requested.
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*) (§ 3(2) G 10 Act). 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). In the GPS case the Court reasoned that electronic tracking is considerably less intrusive than electronic listening, and facilitating the use of the former might obviate the need for the latter (Federal Constitutional Court 12 April 2005; Ross 2005 p. 1807).

Criterion of proportionality
For the use of a (special) means by BfV, a proportionality requirement applies (a *Verhältnismäßigkeitsgrundsatz*). This implies that an infringement of a protected interests of a subject (e.g., right to privacy) is only allowed if this is inevitable (§ 8(1) 3rd sentence BVerfSchG). Further, the law rules that a measure shall not cause a prejudice being recognisably disproportionate to the intended result (§ 8(5) BVerfSchG))).
The BfV has to specify the type of data it requests as well as the time period for which such data are requested and the grounds that justify access to such data. As access to such data is only justified under certain conditions laid out in the law on the BVerfSchG, such specification is necessary as part of a proportionality test. Further, the proportionality requirement is visible in the condition that accessing such data has to be justified in writing and permitted by the Ministry of the Interior which again has to report to the G-10 commission.
For data sharing, the Federal Court noted that transferring personal data to others can result in greater privacy interferences than the actual interference through telecommunications monitoring (Federal Constitutional Court 1999 at 269).

GPS case
In its April 12, 2005 opinion, the *Bundesverfassungsgericht* agreed that the use of GPS technology in police investigations of crimes of considerable importance was constitutional and proportionate (i.e. without a judicial warrant[39]). Although the Court noted that GPS surveillance did constitute an attack on the suspect's personality rights, the extent and intensity of the invasion was not at a level that violated human dignity or the untouchable core sphere of privacy. The Court emphasized the usefulness of GPS technology was limited to revealing a person's location and the length of time spent in a given location, and that GPS did not function effectively in closed rooms or on streets in dense neighborhoods (*GPS case*; Jacoby 2005, p.1088).
Further, the Court found that *Rundüberwachung*, or total surveillance (i.e. multiple simultaneous observations), leading to the construction of a personality profile of a suspect, would be constitutionally impermissible. However, the Court did not find that periodically reading the suspect's mail, tapping the suspect's phone lines, observing his home via video, tracking his car by GPS technology, and limited 'particularly sensitive' acoustic surveillance was at the level of a *Rundüberwachung* (Jacoby 2005, p.1089).

[39] The Generalbundesanwalt successfully argued that in this instance GPS surveillance involved a non "Richter vorbehaltene Maßnahme (BvR 581/01 at 39).

The effective overlap of different surveillance techniques had been small. The investigators used the GPS technology because the suspect was successful in evading observation teams and in disabling other surveillance technologies such as electronic beepers. The police conducted minimal wiretapping since the suspect, who suspected that his phone lines were being monitored, had spoken very little by telephone (Ross 2005, p.1808). Thus, strategies of avoidance by suspects may result in justification for the use of more invasive technologies.

Terrorist profile
One of the 9/11 responses in Germany was to pro-actively find potential terrorists among students enrolling in German universities, among others. Personal data was required to be provided to the authorities (see Achelpöhler et al. 2004). The threatening profile they sought was: male, between 18 and 41 years old, Islamic, student or former student, valid permit of residence without any local restriction, unknown to the police, no children of his own, financially independent (not understandable, irregular deposits in the bank account). This very abstract profile resulted in a total of 31,988 cases. These all appeared in the "Verbunddatei Schläfer", a central database of the state police agencies. The Federal Constitutional Court has ruled that the informational right to self-determination can only be invaded in concrete and significant dangers to Germany or the life and limb of individuals. Preventive measures such as these were ruled to be unconstitutional (see *Rasterfahndung* case).

Monitoring of telecommunications
In 1999, the Federal Constitutional Court took the view that allowing the monitoring of telecommunications in order to prevent the counterfeiting of money abroad constituted a disproportionate interference with the secrecy of telecommunications as protected by Article 10 of the Basic Law. It argued that this danger as such could not be considered to be as serious as an armed attack on the German State, among other dangers listed. The counterfeiting of money should therefore be included only if it was restricted to cases in which it threatened the monetary stability of the Federal Republic of Germany (*Weber* at 29). The G-10 Act has been adjusted accordingly.
Concerning the transmission of telecommunication data processed for national security purposes to law enforcement, the Federal Constitutional Court judged several provisions as disproportionate.

Duty of Care (how to process/ use the data)
Sections 4 and 6 of the G-10 Act provide that personal data obtained by means of monitoring measures about a person involved in the telecommunications monitored has to be destroyed if they are no longer necessary for the purposes listed in the Act and are no longer of significance for an examination by the courts of the legality of the measure. The destruction has to be carried out under the supervision of a person qualified to hold judicial office. The destruction has to be recorded in minutes. It is necessary to examine every six months whether personal data obtained can be destroyed. Access to data which are merely kept for the purpose of judicial review of the monitoring measure, or data necessary for notifying the subject of the monitoring have to be blocked. They can only be used for these purposes (BVL building on Weber).
Remaining data have to be marked so that they will only be used for specified purposes (§1 (1.1) and § 4 G-10 Act).

BfV

For post and telecommunication data the provisions of § 4 of the G-10 Act apply (documenting the goal of data collected, use only in accordance with collection objective, every 6 months review of need to maintain the collected data, documenting removal of data, strict rules on data transfers etc.).
Data management is also arranged in § 14 of the BverfSchG. It rules that the file name, purpose of the file, conditions to be complied with when storing, transferring and using the data, supply or input, access authorization, time periods for reviews, duration of storage, and recording of access must be documented.
The measure shall be stopped as soon as its purpose has been achieved or if there are indications that it cannot be achieved at all or by employing these assets (§ 9(1) BVerfSchG).

Bundesnachrichtendienst
The transmission of personal data, can be performed solely for the purposes which justified the collection of the data (*Zweckbindung*) (§ 4(4)). The receiving organisation can use the personal data only for the purposes for which the data were provided (§ 4(5)).
The execution of the monitoring process as such has to be recorded in minutes. The data contained in these minutes can be used only for the purposes of reviewing data protection and have to be deleted at the end of the year following their recording (BVL building on *Weber 32*).

Available means and required permissions
The BfV, BND and MAD are entitled to monitor and record telecommunications within their own sphere of activities (§1(1) and § 9 G 10 Act, Weber at 19). They submit requests to monitor individuals or for strategic monitoring to the G-10 commission.

BfV
The head of BfV or his deputy shall submit the application for requested information (of § 8a(4) BVerfSchG) and give reason for it in writing, specifying the exact nature, scope and duration of the monitoring measure (§10(2) G-10 Act). For orders concerning individual monitoring the order has to specify the individual concerned, and the phone number or other characteristics of the telecommunication (*Telekommunikationsanschlusses*) (§ 10(3) G-10 Act).
The Federal Ministry commissioned by the Federal Chancellor shall decide on the application and notify the G-10 Commission of the applications granted prior to their implementation on a monthly basis. The G-10 Commission shall decide on the admissibility and necessity of seeking information (§ 8a(5) English version BVerfSchG). The G-10 Commission has to authorize both surveillance measures (§ 15(6) G 10 Act), and measures involving special data categories (BVerfSchG § 8a(5)). In urgent cases, the Minister may obtain *ex post facto* approval (G-10 Act art. 15(6) & art8a(5) BVerfSchG) (building on *Weber at 115*).

The use of an IMSI catcher is only allowed if location data, or EMEI or IMSI data cannot be recovered otherwise or this is significantly more difficult (BVerfSchG § 8a(2) & § 9(4)). Typically, first real-time location data is acquired from telecom providers. Then the IMSI catcher is used to determine more accurately the position of the cell-phone.

Strategic monitoring

As to strategic international monitoring, only the head of the BND or his deputy are entitled to lodge an application for a surveillance order. The application has to be lodged in writing, had to describe and give reasons for the nature, scope and duration of the measure. The parliamentarian Review Commission (PKG) has to consent.

For strategic monitoring, the new G-10 Act does not require to explain that other means of carrying out the investigations either have no prospect of success or are significantly more difficult (§ 5 G 10 Act; §9(3) G-10 Act; cf. *Weber* at 19)

Data category	Data request by	Data warrant by	Legitimacy and proportionality test by
Data from airline companies	Head of the security and intelligence service	Federal Ministry of the Interior	Federal Ministry of the Interior
Data from financial institutes	Head of the security and intelligence service (or servant allowed to hold legal office)	Relevant Ministry	Relevant Ministry
Data from mail delivery companies	Head of the security and intelligence service	Relevant Ministry	G-10 Commission
Traffic data from telecom providers	Head of the security and intelligence service	Relevant Ministry	G-10 Commission (see art.8a(2) no. 4)
Data from tele service providers	Head of the security and intelligence service	Relevant Ministry	G-10 Commission (see art. 8a(2) no.5 BVerfSchG)

Table 10.1 Data categories that may be requested by BfV

Type of data (Law on BfV/ G-10 Act)	Examples	Permission/ Requisition by	Law
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	BfV	§ 8(1) BVerfSchG)
Traffic data	Historical and future location data of cell-phone if actively been used, date and time of use	G-10 commission	§ 8a (2.4, 4, 5 BVerfSchG) & § 9(4) (IMSI catcher)
Content of communications	Content of an email or voice mail	G-10 commission	G-10 Act
Certain stored data: other data	(Historical and future) location data of cell-phone in stand-by mode	N/A	N/A
Data processed after requisition date and directly available to national security and intelligence	Real-time location data of cell-phone if actively been used, real-time standby traffic data	G-10 commission	§ 8a (2.4, 4, 5 BVerfSchG)
Sensitive data (1)	Data concerning racial or ethnic origin, religious or philosophical beliefs, or concerning health or sex life	BfV	§ 8(1) BVerfSchG
Sensitive data (2)	Data concerning political opinions, trade-union membership	BfV	§ 8(1) BVerfSchG

Table 10-2 Sensitiveness of data according to German law applying to BfV

For how long can location information of mobile devices be tracked and traced?

The limit on the duration of monitoring telecommunications measures is three months. The implementation of the measure can be prolonged for a maximum of three months at a time (*Weber at 98* see also § 10(5) G-10 Act). The warrants on special data categories (including telecom data) are equally valid for a maximum of 3 months with a possibility to extent for another 3 months (§ 8a(4) BVerfSchG).

The categorisation of required consent for different activities may imply an order of privacy infringements. With respect to data, the following order was found in the G-10 Act/ BVerfSchG:

- Historical (location data of cell-phone in stand-by mode)
- Home
- Personal communications: Content of an email or voice mail
- One's whereabouts and movements: Real-time location data of cell-phone if actively used AND Historical location data of cell-phone if actively been used (incl. date and time of use)
- Information concerning racial or ethnic origin, religious or philosophical beliefs, or concerning health or sex life, data concerning political opinions, trade-union membership AND Name, address, phone number, kind of service used

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

Monitoring measures of the BfV, BND and MAD are supervised by two bodies, the parliamentary Supervisory Board (Parlamentarische Kontrollgremium, PKG; § 1(2) G-10 Act) and the G 10 Commission for the review of interceptions of private communications (see § 14 and 15 G 10 Act; PKG-Act).

Parliamentary Review Board (PKG)

The *Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Kontrollgremiumgesetz - PKGrG)* provides the framework for the tasks of the parliamentary Review Board. The Board is the controlling mechanism for the activities of the federal security and intelligence agencies. It has the right to access all documents or data of the security and intelligence services, interview servants, visit the services and request information (§ 2a PKGrG). The data cannot be provided if this would prejudice the proper fulfilment of tasks, or if the data that are being stored must be kept secret on account of an overriding justified interest of a third party (§ 2b(2) PKGrG). The Federal Minister authorising monitoring measures has to inform the board at least every six months about the implementation of the G 10 Act (§ 14(1) G 10 Act). The same applies to the implementation of § 8a(2) (on special data categories) with the addition that the Federal Minister shall particularly give an outline of the reason, scope, duration, results and costs of the measures taken (BVerfSchG § 8a (6)). On an annual basis, and in the middle and at the end of one legislative term, the PKG shall - for evaluation purposes - submit a summary report to the German parliament on the implementation of the measures specified in § 14(1) G 10 Act and §8a(2) BVerfSchG (on special data categories) and their nature and scope and the reasons for ordering them (§ 14(1) G 10 Act; BVerfSchG § 8a(6); § 6 PKGrG; Schmid 2001 §9.3).

The parliamentary Supervisory Board consists of nine members of parliament, including representatives of the opposition (see website Bundestag). They are meeting in strict secrecy which they are required to maintain after residing from the commission. The PKG meets at least every 3 months (§ 5(2) PKGrG). The PKG has a five person staff (O'Connor 206, p.342).

G-10 Commission

The G-10 Commission is founded by the G-10 Act. The G 10 Commission decides on the necessity and admissibility of restrictions on the privacy of correspondence,

posts and telecommunications pursuant to Article 10 of the Basic Law as well as on specific data categories as specified in § 8 of the BVerfSchG. The Federal Minister authorising surveillance measures, and measures involving special data categories, has to inform the G 10 Commission monthly about planned monitoring measures and has to obtain its prior authorization (BVerfSchG § 8a(5)). In urgent cases, the Minister may obtain *ex post facto* approval (§ 8a(5) BVerfSchG) (building on *Weber* at 115).

Complaints

Article 19 (Restriction on basic rights) of the Grundgesetz rules that (translation ECtHR in Weber):

> "If a person's rights are violated by a public authority he may have recourse to the courts. If no other jurisdiction has been established, the civil courts shall have jurisdiction."

(*Weber*)

Subjects can claim their personal information to be provided, corrected, or deleted (BVerfSchG § 15 - Auskunftsrecht - § 12 Berichtigung, Löschung). If the BfV does not act accordingly, a complaint can be filed with the Court (*Verwaltungsgericht*). If the BfV refuses to provide access to the personal data, one can turn to the federal data protection agency (*Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BFDI*) (§ 15(4) 3rd sentence BVerfSchG). For G-10 Act measures one can apply to the G 10-Commission.

The G-10 Commission receives approximately 25 complaints per year (O'Connor 2006, p. 345).

10.4.5 Principle 5: guaranteed accuracy of the data for the purposes of use.

The BVerfSchG (§ 12(1-3) text from English version) details the accuracy requirements for BfV:

> (1) Incorrect personal data stored in files shall be corrected by BfV.
>
> (2) Personal data stored in files shall be erased by BfV if their storage was inadmissible or knowledge of them is no longer required for the fulfilment of its tasks. The data shall not be erased if there is reason to believe that erasure would impair legitimate interests of the data subject. In this case the data shall be blocked and shall only be transferred with the data subject's consent.
>
> (3) When dealing with particular cases, BfV shall check within given periods, after five years at the latest, if stored personal data must be corrected or erased.

If it is ascertained by BfV that personal data stored in records are incorrect or if their correctness is contested by the data subject, a note to this effect shall be made in the record or it shall be recorded by some other means. Further, personal data shall be blocked if it is ascertained by BfV in particular cases that without blocking, legitimate interests of the data subject would be impaired and the data are no longer required for the future fulfilment of its tasks. Blocked data shall be marked accordingly; they may no longer be used or transferred. The blocking of data can be repealed if the conditions are not complied with any more (§ 13 (1&2) BVerfSchG English version).

Personal data transmitted to others (within government) needs to be marked and connected to purposes which justified their collection (see BVerfSchG; Weber at 150).

10.4.6 Principle 6: individual participation in the process whenever possible.

BfV
BfV shall provide the data subject, at his request, with information free of charge on personal data stored on him, if he refers to concrete matters and proves to have a special interest in the information which he has asked for (§ 15 BVerfSchG). Subjects of the data warrant have to be notified about its existence as soon as this does not interfere with the objectives of the investigation (BVerfSchG § 8a(4)).
The data cannot be provided if this would prejudice the proper fulfillment of tasks, expose sources or if BfV's knowledge or its modus operandi might be exposed, this would be detrimental to the Federation or a Federal State, or if the data that are being stored must be kept secret in accordance with a legal provision or by virtue of their nature, in particular on account of an overriding justified interest of a third party (§ 15(2) BVerfSchG).
The Federal Minister has to inform the G-10 Commission whether or not persons concerned by such surveillance measures have been notified of them. If the G-10 Commission decides that notification is necessary, the Federal Minister has to arrange for it to be given without undue delay (§ 15(7) G 10 Act; *Weber at 25*). The obligation to provide information does not refer to information on the origin of the data and the recipients of the data transfer (§ 15(3) BVerfSchG).
If the BfV refuses to provide information on a data subject, the data subject must be informed of the legal basis for this decision. He should further be notified that he may appeal to the Federal Commissioner for Data Protection. This Commissioner shall, at his request, be supplied with the information unless the Federal Minister of the Interior determines in a particular case that this would jeopardise the security of the Federation or a Federal State (G-10 Act § 15 (4)).

BND
BND or the recipient authorities has to inform the persons monitored about the restriction imposed on the secrecy of telecommunications as soon as such notification could occur without jeopardising the achievement of the aim pursued by the restriction and the use of the data (§ 12(1) G-10 Act & *Weber*).

However, the Data protection agency has found in 2003 that 75% of the conducted wiretaps violated the law. Law enforcement agencies did not notify the subjects of the wiretap, something they are required to do as soon as this is possible (see Rotenberg et al. 2004). In 2007, the German public broadcast organisation NDR revealed that for the G8-top journalists were being monitored by the police.

10.5 Balancing national security and privacy

Privacy in Germany can be captured by the right to freely develop one's personality. This includes the decision when and within what limits personal data shall be disclosed. Telecommunications data, both the content of the communication and the circumstances of communication (e.g., traffic data) are considered personal data and are explicitly protected by the German constitution (Art. 10). Restrictions of privacy are permitted if these are justified by prevailing public interests. National security may interfere with the right to privacy if this is necessary, and tests of subsidiarity and proportionality are satisfied. It is required to explain that other means of carrying out the investigations either have no prospect of success or are significantly more

difficult. Privacy safeguards are in the independent G-10 commission deciding, prior to the use of a measure, on the need and appropriateness of using special means such as the monitoring of individuals through their telecommunications.
The Federal Constitutional Court found that *Rundüberwachung*, or total surveillance (i.e. multiple simultaneous observations), leading to the construction of a personality profile of a suspect, would be constitutionally impermissible. It is unclear to what extent 24/7 monitoring of telecommunications results in a personality profile of an individual. Government agencies are not permitted to collect telecommunication data that stems from cellphones in the standby mode since this may reveal of pattern of behaviour. A similar reasoning may come to a conclusion that the same applies to the 24/7 monitoring of one's active cellphone use.

Balancing of interests in case of accessing telecommunication data is performed through the law itself (which outlines the conditions under which access to telecommunication data is legal and justified) and the involvement of the independent G 10 Commission. Another control system is introduced through a parliamentary review. Ultimately, one may seek a remedy through the civil Courts.
Federal Constitutional Court (1999 at 304) noted that it must be ensured that the G 10 Commission, in view of the fact that the Fight against Crime Act has considerably expanded the BND's monitoring activities, is provided with the staff needed to effectively fulfill its mission. The current capacity of the review and control commission may be insufficient provided their legal tasks. The capacity of the only commission that is pro-actively reviewing the security and intelligence agencies, PKG, is currently five staff members.

Effectiveness of current means available to protect national security
The 1994 amendments to the G 10 Act considerably extended the range of subjects in respect of which so-called strategic monitoring could be carried out. Whereas initially such monitoring was permitted only in order to detect and avert the danger of an armed attack on Germany, now also allowed strategic monitoring in order to avert further serious offences (*Weber* at 114 referring to § 3(1) of the G-10 Act). Since 2001, legislative changes were accepted to target extremist and terrorist organisations broadening the scope of permissible actions for federal security and law enforcement agencies including increasing information sharing between agencies (O'Connor 2006, p.338).
The latest development is the implementation of the Data Retention Directive in German Law. It attracted strong criticism (see website Vorratsdatenspeicherung). For example, the former Minister of Justice Leutheusser-Schnarrenberger warned for developments towards a '*Uberwachungsstaat*' (total surveillance state) (Zwaap 2007). The German implementation of the Data Retention Directive requires to store data on who has contacted whom via telephone, mobile phone or e-mail for a period of six months. In the case of mobile calls or text messages via mobile phone, the user's location will also be logged, and anonymising services will be prohibited (website Vorratsdatenspeicherung).
The effect of the 1994 and 9/11 measures and also the prospect of the data retention directive measures have not been assessed or reviewed. In a survey study of the *Bundeskriminalamt* (Mahnken 2005) asking the Bundeskriminalamt, Ministry of Justice and Ministry of the Interior about unavailable traffic data which might have been useful in criminal proceedings, 381 cases were reported. The value of this number remains unassessed since of the 6.4 million criminal proceedings in 2005, 2.8 million remain unresolved (see BKA 2005; see also website Vorratsdatenspeicherung 2).

As in Canada, the number of interceptions by law enforcement are published (required by par. 110 TKG). This contributes to the transparency of the use and effectiveness of government operations. It provides some indication of the size and frequency of the use of special means. Significant increases or diminished use of special means may readily be accessed and used by members of parliament. Uncertainty on the number of special means, gives raise to speculation and a possibly unfair frightening prospective.

11 Balancing privacy and national security needs and interests

Both privacy and national security are concepts that are difficult to capture. Despite the difficulties to establish exact boundaries around privacy or national security several conclusions from the literature review can be drawn.
First, in western societies, the limited access approach is commonly used as a concept to understand privacy. This approach emphasizes the autonomous individual, choice and control, and social relationships as voluntary or as barriers to independence. The control over access to self and over the information about someone are central. The extent to which individual's privacy needs are satisfied depends on a variety of factors: the context, culture and the individual's perception of privacy, amongst others. Privacy is not an absolute right, however. Other interests may interfere with the right to privacy. This does not imply that any purpose may interfere with the privacy right.
For the level of location privacy, the type of location data, the context of the information available, and the timeliness of the information are decisive. The use of highly detailed (e.g., scale 1:500), real-time location data linked to a sensitive context, such as a church, can generally be expected to be at a higher 'privacy level' than less detailed data (e.g., scale 1:25,000) of a decade ago without a link to a specific sensitive context.
Directive 2002/58/EC distinguishes two types of location data as part of the traffic data and location data. Traffic data are data that are required to enable the communications and those required for the billing process. It includes the phone numbers, duration of communication, time of communication and also information on the location of the cellphone at the time of calling (i.e. at the start and termination of the connection). Location data of a mobile device are traffic data because they are necessary to enable the transmission of communications (recital 35 Directive 2002/58/EC). The other location data are location data that are not necessary for the transmission of communications, and which are typically more accurate than traffic data.
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 and Kamerstukken 25877, nr. 58; UN Economic and Social Council *Siracusa Principles* (article 29)). 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*).[40] As a practical fact, absolute privacy is difficult to accomplish, but absolute security may be as problematic to reach (see AIV 2006, p.8).
Starting point in this chapter 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.

11.1 Balancing national security and human rights

States may need "to take measures to protect the fundamental rights of everyone within their jurisdiction against terrorist acts, especially the right to life" (art. 1 Guidelines EU 2002). Typically, these measures may be those performed by security

[40] In this respect, it has been recommended to establish a requirement that if it is suggested that national security is threatened this is supported by actual circumstances or a certain rate/index of specific notion or suspicion to prevent that states can too easily do as they like (see Loof 2005, p.339; Koops et al. 2005 p.188).

and intelligence services to protect the national security. In this respect, national security and human rights are not conflicting, but complementary to each other.

The Charter of the United Nations may be exemplary for the discussion on balancing human rights with security interests (see website UN). On the one hand it promotes peace and security (in article 1.1):

> "To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace"

On the other hand, it is also one of the UN's key purposes to promote and encourage human rights (article 1.3):

> "To achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion"

> "In a given instance, a balancing regulator needs to judge whether a data subject's rights (or at least, claims) outweigh the interests of the data user, without bringing to bear a range of particular knowledge about the contending parties. This is a difficult judgement, even in the abstract. But in another sense - and this may be especially so when regulators seek to frame preventative policies, or to influence the development of technologies – balancing requires not only a conception of rights and legitimate interests, but some grasp of the distribution of hazards and fears as well. Because privacy rights do not necessarily prevail over other interests, without such knowledge it may be difficult to argue against data users' persuasive demonstration of the known and possibly measurable (or costable) harm to their activities if their use of personal data were restricted."
>
> Raab and Bennett (1998, p.265-266)

What is the proper balance between national security and privacy? (O'Harrow Jr. 2005, p.13; Westin 1967; Margulis 2001; Altman 1975; Levi et al. 2004; Walters 2001). In the next section, we will use the six balancing principles as a starting point for further developing a balancing framework for national security and privacy interests. Before we move towards the balancing part, first we discuss the most relevant parties that are or may be involved in the balancing process.

11.2 Parties involved in balancing privacy and national security

Balancing of privacy and national security interests may be accomplished by many parties. Here we address: the user of the mobile device, the telecom provider, the security and intelligence service, and an independent authority.

11.2.1 User

Users may use (a) strategies of avoidance or (b) use preventive technologies to circumvent government surveillance. Technology may allow users to choose through privacy enhancing technologies (PETs) not to be traced or tracked. For mobile devices one may think of a Faraday cage which prevents radio waves entering or leaving ensuring no surveillance, but also disabling any communications (see Wheeler 2004). If one still wants to communicate one may use an information diffusion approach to scatter the user's location information to confuse the attacker (Lee et al. 2005, p.1007), or use frequently changing pseudonyms (Wong et al. 2005, p.83). Use of encrypted and anonymously purchased mobile phone communications between offenders make both them and their content difficult to trace (IPTS 2003, 180).
Although these PETs do protect the content of the communication, this excludes the location of the device. Since the availability of the location information is a prerequisite for using the functionality of the mobile device, it cannot be encrypted or otherwise withheld from intelligence or law enforcement agencies in the instance that these have a legal mandate to access the location data. Therefore, these PETs may be sufficient to guard against private intruders, for law enforcement and intelligence services they may not.
In addition, encrypted data can be deciphered and anonymous identities can be deanonymised, even when they are in the hands of trusted third parties/ intermediaries. Often those who developed these deciphering technologies are working for or cooperating with intelligence services.
In the context of this research, users of cellphones are no party in the balancing privacy and national security interests.

11.2.2 Telecom provider

To a certain extent telecom providers may be required to balance different interests of the data they process. This may be true for data requests from marketing companies that aim to target cell-phone users for a specific product.
For national security purposes, telecom providers often do not have a choice: they need to provide the data on request. Legislation on telecommunications may further require the ability of telecom providers to cooperate with security and intelligence services. For example, telecom networks may be required to be fit for placing government wiretaps. And legislation may require them to store all telecommunications data for a five year period. In other countries these requirements may not exist, allowing the telecom provider a lot of freedom in its operational activities.

Depending on the situation in each individual country, the extent to which national security protectors can take advantage of the telecom providers varies with the legal requirements for telecommunication and the legal powers of the security and intelligence services.

11.2.3 Security and intelligence service

Security and intelligence services are often the first to identify a potential threat to the national security. Further action may be necessary. The security and intelligence service is likely to decide on further action. The initial decision to process further with a threat is in the security and intelligence service. Based on the threat analysis and the urgency of the threat, they may decide or propose to start an operation.
The ECtHR warns that allowing secret surveillance poses a threat of undermining or even destroying democracy on the ground of defending it (*Klass*). Therefore, it is recommended or required to have sufficient safeguards in the decision-making process

preventing misuse of the law to the greatest extent possible. These safeguards can be the involvement of independent authorities in the decision-making process, or independent review of the execution of the mandate.

11.2.4 Independent authority

It is key that the principles developed by the ECtHR are being adhered to to the greatest extent possible. It is evident that some form of oversight or review is required to meet this requirement.
Independent authorities may also take part in the decision-making process before the decision is executed. Such an ex-ante involvement is found in Germany and Canada. Also in law enforcement in the Netherlands, a judge assesses the balance of human right interests and criminal investigations interests.

11.3 Balancing through six balancing principles

In chapter three we developed six balancing principles that were the basis for the case-studies. The principles were:

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.

Principle 5: Guaranteed accuracy of the data for the purposes of use.

Principle 6: Individual participation in the process whenever possible.

In this section, we will summarise the extent to which the cases adhered to the principles, and how they gave interpretation to the principles.

11.3.1 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.

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 is mandated to collect, analyze, and retain information and intelli-

gence 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 cases, the law is accessible to all.

Means of interference foreseeable
Legislation provides 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 has balanced to a certain extent the needs of society and those of individuals.
In section 11.3.2 a categorisation of telecom data is provided based on the authority that needs to approve the data acquisition. This categorisation by law is also used in criminal law: for a serious crime, e.g., a kidnapping, more intrusive means are available than for minor crimes, e.g., shop lifting.

Intelligence and security agencies in the cases have a bucket full of available means that may be utilized to address concerns of national security. The collection of information is among the core businesses of these agencies. This may be accomplished through publicly accessible sources such as newspapers, internet, television, and other published materials. Also members of the public, other government agencies, and other intelligence agencies may be sources. An intelligence and security agency may collect information actively through the use of infiltrators, technical interception of (electronic) equipment (e.g., wire-taps) and electronic surveillance of targeted persons or places (e.g., placing 'bugs'). Only one of these means is information available from telecommunications. And location data is only one type of data available from telecommunications.
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 of this section).
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, 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 can.
However, strictly reading the EU Directive 2002/58/EC, telecom providers in the European Union are not required to store location data (or the location data part of

traffic data) if the communication is within a country. For the billing purpose, the traffic data can even be limited to the fact that the BTS was in one country instead of documenting data from a specific BTS. Directly after the notification that a cellphone called from a specific country, the more detailed location data can be removed. In cross-national communications it is necessary to document these detailed data as long as the fees vary from country to country. But also here the knowledge that the cellphone was calling from a specific country would be sufficient to satisfy the billing requirement. The Data Retention Directive (2006/24/EC), however, requires European Union Member States to store traffic data for at least six months.

For transparency requirement it should be noted that 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 from each other, both national and international, confirmed that increased transparency promotes the use of infringing means. Affirmation of this hypothesis would argue against the ECtHR requirements.

11.3.2 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). In her methodology of balancing different fundamental rights, Gerards (2006), suggests that also for balancing privacy and national security an equilibrium exist or can be accomplished. 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. Several relevant steps in the balancing process can be distinguished (see Figure 11.1):

- 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.

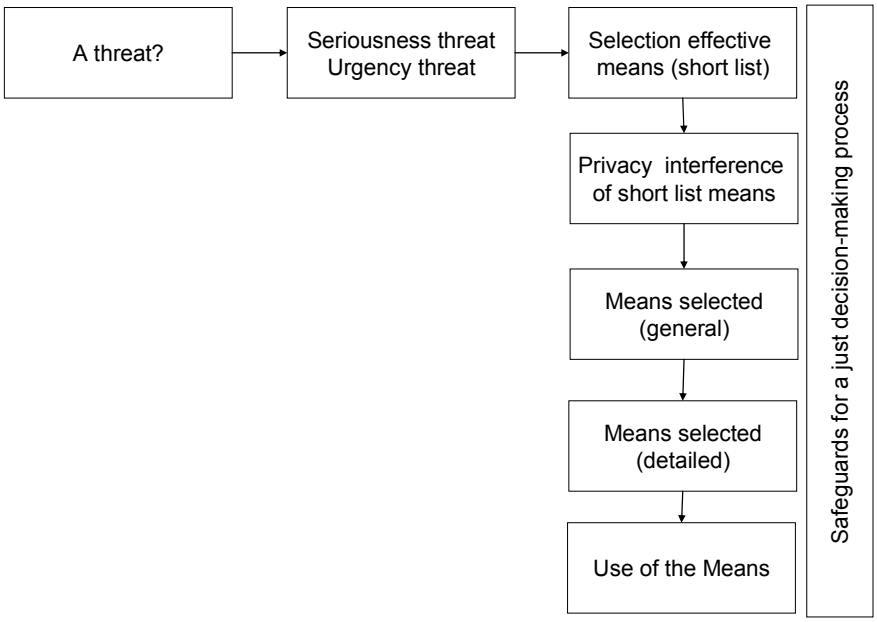


Figure 11.1 General process of balancing national security and privacy for telecommunication

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

In this principle it is assessed whether the selected means and data and proportionate to the legitimate aim. The first step is to assess the availability of means that can effectively address the threat. Or more specific in the context of this research: when is location data of mobile device of use to protect national security interests?
The following table provides some insight in when location information may be useful for the national security interests. It shows that in the first place it is complementary to traffic data to reveal a network of those suspected of threatening national security. 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.
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. It should further be noted that we are here discussing the location of the cell-phone. This implies all kinds of (potential) inaccuracies in the data acquired (see chapter 6). This will result in (unacceptable) uncertainties in decisions based on these inaccurate data.

	Contributes to	Contributes to		In combination with
Content of communications	Reveal network of organisation	Reveal relation between people and hierarchy in network	Link content to activities threatening national security	Observation to verify identification data
Real-time location data (highly detailed) Real-time traffic data (including rough location data)	Reveal network of organisation	To prevent/ stop activity	Link location to activities threatening national security	Tactical information[41] Observation to verify identification data & location data
Historical location data (active use, including stand-by location data)	Reveal network of organisation		Link location to activities threatening national security	Tactical information Observation to verify identification data & location data
Traffic data	Reveal network of organisation	Reveal relation between people and hierarchy in network	Link location to activities threatening national security	Tactical information Observation to verify identification data & location data
Identification data	Link cellphone to user			Traffic data, Observation to verify identification data (who is the user)

Table 11-1 Mobile device data and use for national security purposes

Effect of location data in law enforcement

The identifying information of a cell-phone and the traffic information (who is calling who) are more important for law enforcement than the precise location data. Historic traffic data is critical to reveal connections between suspects (Rotterdamse Politie 2003, p.5). Location data as part of the traffic 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).

[41] Tactical information may be information of relatives, friends, for example, their address.

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 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.

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 the social and political developments (Nouwt et al. 2004, p.354).

Effectiveness of means and subsidiarity

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. In the Netherlands, the total number of new tap orders for 2007 is likely to be in the range of 25,000 phone numbers. This equals 151 taps per 100,000 citizens. In Canada, the number of interceptions of telecommunication has dropped from 1679 interceptions in 2002 (5.2 per 100,000 citizens) to 584 interceptions (1.8 per 100,000 citizens) in 2005. In 2006, the number of taps in Germany on cellphones was 35,816, and approximately 5,000 taps on traditional phones. This amounts in approximately 50 taps per 100,000 citizens. Figure 11.2 shows the differences.

These differences are difficult to explain, and raises the question whether some countries may relatively easy approve, without truly considering its effectiveness compared to other means, the use of one of the most privacy-intruding means: the phone tap.

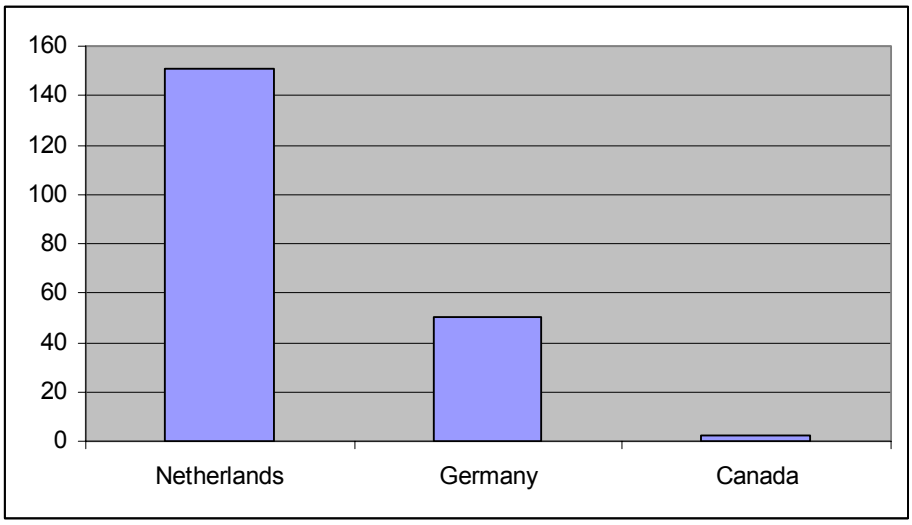


Figure 11.2 The approximate number of taps for law enforcement in the case-study countries per 100,000 citizens

Telecommunication data and privacy

Based on research of the value of location data, the categorisation of personal data in legislation, and studies aiming at categorising different types of personal data, one may come to a general order of sensitivity for data (from most sensitive down):

1. sensitive data: Data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or concerning health or sex life and data in the category of the content of communications (letter, email, voice-mail, phone conversations);
2. real-time data (location, financial transfers);
3. historical location data of cell-phone; traffic data of cell-phone; details about savings, earnings, court judgments, credit ratings, one's visitors, and medical history;
4. education and job history, what one buys, club membership, TV viewing, newspaper reading, and age;
5. identifying data; data that determine the identity of individuals and that connect people and situations: name, address, sex, birth date, administrative characteristics such as phone number, bank account number, client number, license plate number.

These categories can be further specified with respect to the level of detail of the information, the type of data, the timeliness of the data, and the context in which the information is used (see chapter 4).

The processing of location information is typically in the general personal information category. However, if it is linked to a sensitive context or if it is tracked and traced real-time it should be categorized as sensitive personal information. 'Historical' location information would be within in the general personal information category (see chapter 4).

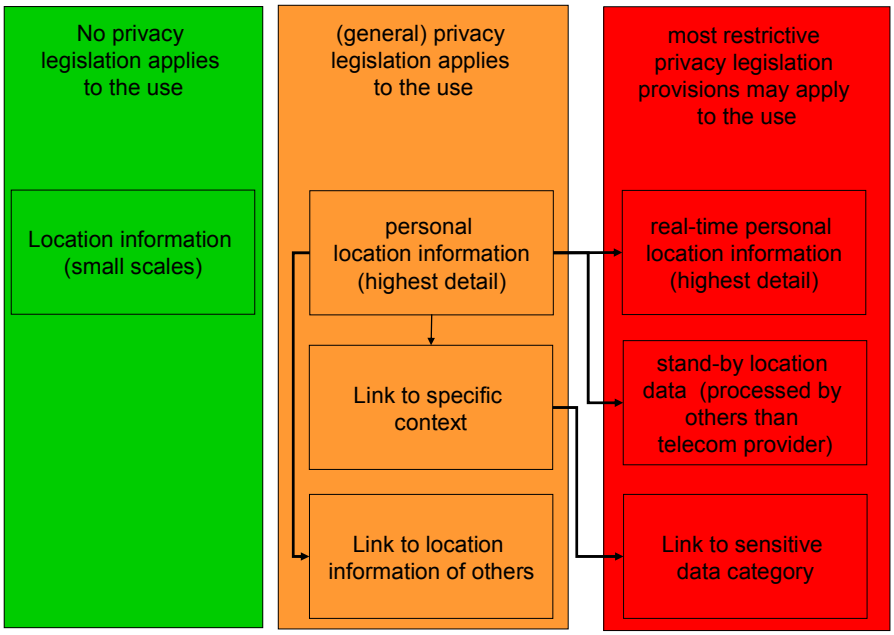


Figure 11-3 Categorisation of location information and applicable legal regime

In a general sense, the use of highly detailed (e.g., scale 1:500), real-time location data linked to a sensitive context, such as a church, can generally be expected to be at a higher 'privacy level' than less detailed data (e.g., scale 1:25,000) of a decade ago without a link to a specific sensitive context.

Aspects of proportionality

The decision whether a selected means or data 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 2004-2005, p. 37):

- 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?

Figure 11.4 shows this graphically.

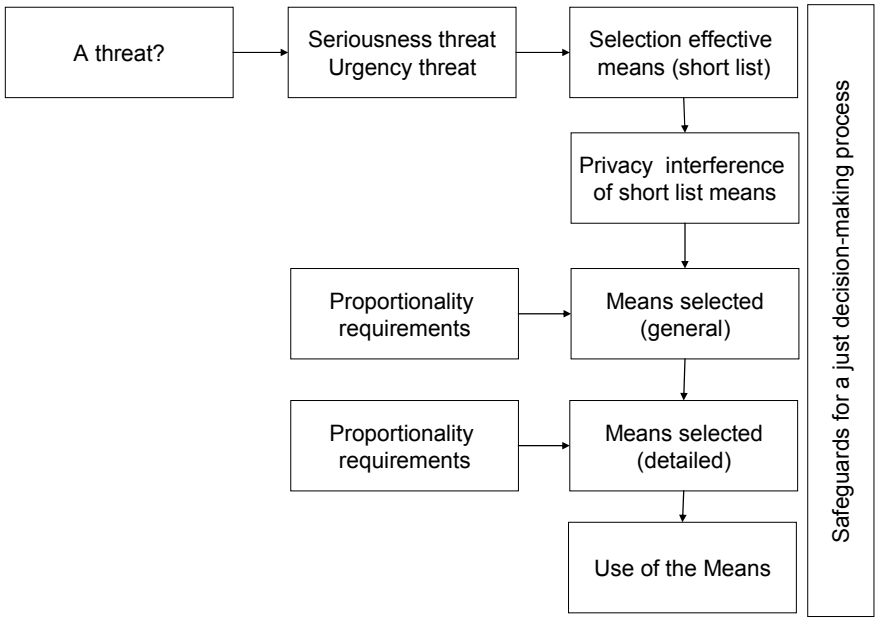


Figure 11.4 General process of balancing national security and privacy for telecommunication including proportionality requirements

Proportionality aspect of using means	Netherlands	Canada	Germany
Effectiveness	yes	yes	yes
Pressing need/ urgency	yes	yes	yes
Place involved in observation	yes	yes	yes
Consecutive period of observation	yes	yes	yes
Intensity of observation	yes	yes	yes
Inconvenience for suspect	yes	yes	yes
Accuracy of data (level of geographic detail)	no	no	no
Timeliness of data	yes	yes	yes
Required effort from telecommunication providers	yes	-	-
Cost	yes	-	-

Table 11.3 Proportionality aspects considered in case study countries

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 may justify the use of more privacy intruding techniques or data. 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. 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 may be used to assess the privacy impact of several selected effective means.

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

Key of privacy protection is a just decision-making process and proper execution of the national security mandate. If the quality of the 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 offenses they seek to punish" (Westin 1967, p.332). AIV (2006, p.52) states 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 Doc. E/CN.4/2005/13 par. 13-15). Concerning wiretapping, Westin found already in 1967 that an independent authority (e.g., a court) order was required to authorize a wiretap (Westin 1967, p.181/2). In the cases, we see that independent authorities may have different roles. Figure 11-5 provides this in the conceptual decision-making process.

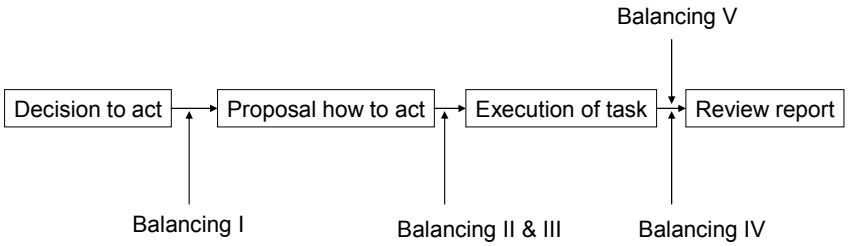


Figure 11-5 Conceptual view of decision making process

Balancing I: initiative to start the process for us 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/ review of activities of intelligence and security agency
Balancing V: continuing overall active review of the operations of the intelligence and security agency

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 II 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).
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). These,

however, cannot render legally binding decisions. In all cases, complaints on the execution of the tasks may (ultimately) be directed at a (civil) court.
Balancing V involves review for evaluation purposes. This will keep security and intelligence services sharp and as a result may improve the decision-making system. Such an independent authority is required to oversee the execution of the activities of the security and intelligence services (Schmid 2001 §9.3). 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). Review by an independent commission is found in Germany, Canada, and for the security and intelligence services in 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 11.4). In law enforcement in the Netherlands such a permanent review commission is non-existent. Special commissions may be set-up by Parliament such as the Parliamentary review commission Van Traa in 1994. This commission was tasked to review the Methods for Criminal Investigations (*Parlementaire enquêtecommissie opsporingsmethoden*). This is, however, an exceptional instrument to use.

	Balancing I	Balancing II	Balancing III	Balancing IV	Balancing V
Netherlands (national security)	Intelligence and Security Service	Intelligence and Security Service	Intelligence and Security Service	Ombudsman, Review Commission, Court	Independent review + parliamentary review
Netherlands (law enforcement)	Law enforcement officer	Public Prosecutor	Magistrate (Court)	Court	-
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

Table 11-4 Balancing for use of real-time location information of mobile devices (active use; the darker the cell, the more independent the balancing)

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, keep pace with developments in the national security sector to fulfill the review task adequately.

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

Table 11.5 summarises the required authority that needs to approve the requisition of telecommunication data for 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. In Canada, the expectation of privacy in private areas, i.e., the home, is greater than in public areas. 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. 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, 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.

Type of data	Examples	NL: Decision/ Requisition by[42]	NL: Decision/ Requisition by[43]	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	Law enforcement office	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	Public Prosecutor	Minister & Federal Court judge	Minister & Independent commission
Content of communications	Conversation, content of an email or voice mail	Minister	Magistrate	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	Magistrate	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	Magistrate	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)	Magistrate	Minister & Federal Court judge	Head of security and intelligence service
Sensitive personal data (2)	Data concerning political opinions, trade-union membership	Intelligence agent	Magistrate	Minister & Federal Court judge	Head of security and intelligence service

Table 11-5 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)

[42] for national security and intelligence agency
[43] For law enforcement

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. 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.

11.3.5 Principle 5: Guaranteed accuracy of the data for the purposes of use.

In the Netherlands, the WIV 2002 requires that the data processing is careful and adequate. Metadata accompanies the data to indicate the reliability of the data or the source of the data. Further, the AIVD should take care of adequate facilities to ensure that the data processed are correct and complete.
In Canada, the CSIS Act does not specify specific requirements concerning the guaranteed accuracy for the purposes of use of the data. This requirement may be taken into account by the judicial control.
In Germany, the BVerfSchG requires to link the acquired data to the objective of the acquisition. It further details requirements for correcting incorrect personal data.
The Netherlands has the most detailed requirements in this respect. This, however, does not guarantee adherence to the legal requirements. Both the Commissie bestuurlijke evaluatie AIVD (2004) and the AIV (2007) criticised the AIVD for this aspect.

11.3.6 Principle 6: Individual participation in the process whenever possible.

Individual participation in secret personal data processing is difficult to establish. In the Netherlands, people can request information about which personal data, if any, is being or has been processed by the national security and intelligence service. The responsible Minister decides that requests for information on processed personal data are denied if data concerning the requestor are being or have been processed, unless:

- the data concerned was processed more than five years ago;
- there are no new data added;
- the personal data are irrelevant for current investigations.

In Canada, individuals are withheld from participation in the process, except for complaints on activities of CSIS. Individuals will not be informed of their communications being intercepted, even if this would not harm any CSIS operations. This information can be withheld as long as the information came into existence less than twenty years prior to the request.
In Germany, the BfV shall provide the data subject, at his request, with information free of charge on personal data stored on him, if he refers to concrete matters and proves to have a special interest in the information which he has asked for. Subjects of the data warrant have to be notified about its existence as soon as this does not interfere with the objectives of the investigation. The data cannot be provided if this would prejudice the proper fulfillment of tasks, expose sources or if BfV's knowledge or its modus operandi might be exposed, this would be detrimental to the Federation

or a Federal State, or if the data that are being stored must be kept secret in accordance with a legal provision or by virtue of their nature, in particular on account of an overriding justified interest of a third party.

Both European cases provide access to individual records if these are irrelevant for the investigations, while in Canada such access would not be provided.

11.4 Privacy enhancing architectures

Developments in technology are expected to result in hybrid systems that incorporate a location identifying component. We foresee developments towards the integration of location information available within WiFi networks, RFID networks, cellphone networks, together with active GPS in mobile devices. Although we might be several years from full integration of these networks, these potentially allow the permanent identification of individuals within a range of a few metres. It is almost impossible not to use devices attached to these networks since we then choose not to participate in modern life. The development of a true privacy enhancing technology that provides the user full control over his devices regarding location information would be the challenge for location technology research. Directions for balancing privacy interests with other interests of society may be found in non-centralised storage of information. Such privacy-preserving directions are, for example, developed for the Transport Information Monitoring Environment (TIME) (Evans et al. 2007). In addition, hybrid systems such as using WiFi for VoIP and a mobile device, the WiFi router only needs to know that a mobile device wants to use VoIP. Since VoIP is free there is no need to process the identifiers of the mobile device. In this way, hybrid systems may be not only a big threat to privacy, but also the privacy savior of the future.

In the instance of the Dutch public transportation chipchard (*OV-chipkaart*), privacy issues were addressed at the final stages of the implementation. It was only after the opinion of the Data protection agency that it was truly considered to be important to address. However, it was not very timely provided the significant investments already made; it would be too costly to make the system more 'privacy-friendly'.
For road-pricing (*rekening rijden*), a similar development may be followed in the Netherlands. In an early stadium privacy issues were mentioned and several organisations have recommended a privacy enhancing architecture of decentralised databases that automatically erase personal data after the bill has been paid (see, for example, Eras 1998).

11.5 Summary

In balancing national security and privacy several relevant balancing steps can be distinguished. First the threat and its urgency need to be assessed. Then the available and expected effective means explored. One of these means may involve telecommunications. In the decision to use an effective means, the privacy impact should also be considered.
It is difficult to compare in a general way telecommunications with other available means with respect to privacy interferences and effectiveness. Likewise, the privacy impact of the use of telecommunication data is very context, time and type depending. Therefore, it should be decided on a case-by-case basis whether telecommunication data are the most effective means and which telecommunication data are the most effective data to address the threat. In this respect, the least detailed legislation

(Canada) is assessed to be the balancing framework that most adequately will respect the totality of the circumstances which are key in determining the level of location privacy.

Provided the context-specific characteristics of both the effectiveness and the level of location privacy of telecommunication data, the decision-making process is key to arrive at a fair balance between privacy and national security. The requirements of proportionality and subsidiarity are similarly fulfilled in the case-studies. In this respect, similar aspects are considered in the decision to use a privacy interfering means. However, for the final decision to use a special means interfering with the right to privacy, only the security and intelligence agency in the Netherlands can do this without involvement of an independent authority. Safeguards in the Netherlands are established in the overall pro-active tasks of the review commission, among others.

Westin (2003) on balancing privacy and other interests of society

"[D]ebates over privacy are never-ending, for they are tied to changes in the norms of society as to what kinds of personal conduct are regarded as beneficial, neutral, or harmful to the public good". "We can hope that the institutional mechanisms our society uses to control investigative excesses will be applied. These include active judicial oversight of surveillance systems, civil liberties and privacy group studies and advocacy, media exposures of surveillance-system violations and investigative wrong-doing, continuing executive-agency reviews of working procedures, and legislative investigations resulting in installation of effective legislative safeguards. None of this will be easy"

12 Conclusions

This research centralised around the question:

"How should the right to location privacy of users of mobile phones and other terminal equipment be balanced with the tracing and tracking interests of the (national) security sector?"

The general concept of privacy, national security and the feelings with regard to their balancing were applied to the specific issue of location privacy, and more specifically to the tracing and tracking of mobile terminal devices by public authorities. This chapter presents the main findings for each of these aspects.

12.1 General concept of privacy and its perception

Privacy exists and performs in many shapes and sizes. Although some, mostly privacy scholars, warn for the impact of the loss of privacy, many citizens ignore these warnings, either because they are ignorant, unaware, or unable to oversee the consequences of the loss of something that remains a vague concept and which does not need to protect those that have nothing to hide.
Despite the difficulties to establish exact boundaries around privacy several conclusions can be drawn from the literature review.
In western societies, the limited access approach is commonly used as a concept to capture privacy. This approach emphasizes the autonomous individual, choice and control, and social relationships as voluntary or as barriers to independence. The control over access to self and over the information about someone are central. The extent to which individual's privacy needs are satisfied depends on a variety of factors: the context and the individual's perception of privacy, amongst others.

The extent to which the use of location information interferes with the right to privacy depends on the type of information, the level of detail of the location information, the timeliness of the information, and the context to which it is linked. As a consequence, the extent to which location information can be considered personal data or sensitive personal data varies from situation to situation. For example, concerning telecommunication data, Directive 2002/58/EC distinguishes two types of location data: traffic data and location data. Traffic location data is necessary to enable the communication. 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. However, linking traffic data to a specific context and time (who did you call yesterday at 8pm) may change the non-personal traffic data into personal information to which privacy restrictions applies. In a general sense, the use of highly detailed (e.g., scale 1:500), real-time location data linked to a sensitive context, such as a church, can generally be expected to be at a higher 'privacy level' than less detailed data (e.g., scale 1:25,000) of a decade ago without a link to a specific sensitive context. It is the totality of the circumstances that determine whether location privacy is at stake.

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 con-

versation 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.

Experimental research on telecommunication use and location based services suggest that people generally do not value location privacy as high as one may expect. At least, they do not act as if they value their location privacy. Walters observation may also apply to location privacy: Generally privacy's importance is not recognized by individuals "until it is taken away… [..]" (Walters 2001, p.8).

12.2 Concept of national security

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. National security is an extremely flexible notion, however. It is difficult to assess whether something or someone is a threat to the national security. The interpretation of the concept may be different from society to society, culture to culture and may change throughout time.
Many means may be used to protect the national security. Physical, and data surveillance are among these. There are many examples available that show that these means can be effective. However, there are many aspects that need to be taken into account in using these means (e.g., accuracy of processed information, interpretation of the data, competence of intelligence services).
Decisions based on the processed data may have a great impact on individuals and eventually on society. Sufficient safeguards should be in place to ensure to the greatest extent possible that it is only national security that is protected, not another interest, and that the use of the means protecting national security are strictly limited to what is listed in the task to which the means were assigned.

12.2.1 Role of technology

A wide range of privacy enhancing technologies are available. Location technology does provide security and intelligence services with the means to track and trace individuals at varying levels of accuracy. Especially hybrid equipment, using both cellphone technology and navigation technology allow for increased positioning of mobile equipment.
However, since the availability of the location information is a prerequisite for using the functionality of 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 intelligence services they may not. Thus, relying on technology alone to protect individual's privacy may be insufficient. The balancing has then be left to a decision in the extent to which technological advances may be used for national security purposes.

12.3 Balancing national security and privacy

This chapter provides the findings of the study of relevant national and international legislation and case law. The United Nations, OECD and European privacy regimes clarify that privacy is a fundamental right, but may be invaded by other rights that serve other (more absolute) objectives of general interest recognized by a society. The right to privacy is in most international treaties recognized 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. An analysis of the European Convention of Human Rights, Convention 108, OECD principles, European Union Directives, judgments of the European Court of Human Rights resulted in six general principles that need to be satisfied to interfere with the right to privacy for purposes of national security (see also Westin 1967, p.370):

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.

Principle 5: Guaranteed accuracy of the data for the purposes of use.

Principle 6: Individual participation in the process whenever possible.

Adherence to these principles was sought in four case-studies: the Netherlands, Canada and Germany for national security interests and finally law enforcement interests in the Netherlands.

Balancing stages

In balancing national security and privacy several relevant balancing steps can be distinguished. First the threat, its seriousness and its urgency need to be assessed. Further, from 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.

Intelligence and security agencies in the cases have a bucket full of available means that may be utilized to address concerns of national security. The collection of information is among the core businesses of these agencies. This may be accomplished through publicly accessible sources such as newspapers, internet, television, and other published materials. Also members of the public, other government agencies, and other intelligence agencies may be sources. An intelligence and security agency may collect information actively through the use of infiltrators, technical interception

of (electronic) equipment (e.g., wire-taps) and electronic surveillance of targeted persons or places (e.g., placing 'bugs'). Only one of these means is information available from telecommunications. And location data is only one type of data available from telecommunications.
It is difficult to compare in a general way telecommunications with other available means with respect to privacy interferences and effectiveness. Likewise, the privacy impact of the use of telecommunication data is very context, time and type depending. Therefore, it should be decided on a case-by-case basis whether telecommunication data are the most effective means and which telecommunication data are the most effective data to address the threat. In this respect, the least detailed legislation (Canada) is assessed to be the balancing framework that most adequately will respect the totality of the circumstances which are key in determining the level of location privacy.
Provided the context-specific characteristics of both the effectiveness and the level of location privacy of telecommunication data, the decision-making process is key to arrive at a fair balance between privacy and national security. The requirements of proportionality and subsidiarity are similarly fulfilled in the case-studies. 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. Use of most intruding means would typically be reserved for most urgent threats.
However, for the final decision to use a special means interfering with the right to privacy, only the security and intelligence agency in the Netherlands can do this without involvement of an independent authority. Safeguards in the Netherlands are established in the overall pro-active tasks of the review commission, among others.

Effective remedy and adequate safeguards
An effective remedy should be considered as key to privacy protection. An effective remedy is generally considered to include:

- well developed procedures within the security and intelligence services in arriving at a decision to use special authorities;
- well developed procedures to execute the decision;
- involvement of independent authority in the decision to use special authorities (ex-ante);
- independent oversight (ex-post);
- decision powers to interfere in the operations of the security and intelligence service for the independent control mechanisms, and
- preferably with intern oversight by a privacy commissioner/ inspector.

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 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).
In all cases, complaints on the security and intelligence agencies should be filed with the security and intelligence agency's review commission. These, however, cannot render legally binding decisions. In all cases, complaints on the execution of the tasks may (ultimately) be directed at a (civil) court.
Review by an independent commission is found in Germany, Canada, and for the security and intelligence services in 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.

Approval for using location data varies from country to country. 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. In Canada, the expectation of privacy in private areas, i.e., the home, is greater than in public areas. 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. 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.

Effectiveness of using location data of mobile devices
Location information of telecommunications is only one of the available means for national security. Location data as part of the traffic 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). Real-time location data may help to prevent someone going somewhere, but only in combination with physical surveillance. In the future, this surveillance may be through under-the-skin-electronic-chips, or bracelets controlled at a distance.
Often less private information is more useful to national security objectives than location data. It is questionable how proportionate tracking someone is since it may result in an almost complete picture of someone's life, especially in combination with other information. Provided the limited additional information real-time location adds to the national security objective, it should be claimed and used to the minimum.

12.3.1 Other findings from the case-studies

Money as privacy's savior
Privacy is currently protected by economic arguments: telecom providers refuse to store the minimum of data no longer than necessary. Due to the cost of storing data, they do not keep records of standby data of a cellphone. In Jamaica, road centreline and parcel data maps are assessed to be crucial to 24/7 monitor the movements of persons on parole, but the national mapping agency refused to provide these to the private company contracted by government to monitor (Walker 2007).
This economic argument is a very fragile basis for the protection of privacy.

Transparency of law against privacy interests!?
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 cir-

cumstances (i.e., crimes) the more likely it is that these means are being used for these specified circumstances. Several interviewees independent from each other, both national and international, 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.

Reporting use and effect of available means

To assess the effectiveness of available means, qualitative or quantitative data on the use and effect of these means are a prerequisite. In Canada and Germany, general data on the number of phone taps placed by law enforcement per year are reported as a legal requirement and publicly available. In Canada these are also available for the security and intelligence agency. Unlike these countries, in the Netherlands the security sector, nor law enforcement is required to report these facts. Accordingly they, or the Minister cannot be held accountable for increases or decreases of the number of request for these data. Very recently (May 2008), the Minister of Justice revealed that on a daily basis 1681 tap orders are executed. This suggests that either a significant part of law enforcement is involved in the tapping business, or that a significant part of these taps is placed without being used. The latter situation would imply a disproportionate interference with the right to privacy. The reveal is likely to attract the attention of members of parliament which have now a basis to question the effectiveness of the used means, especially compared to other countries.

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.

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.

12.4 Role of Technology in balancing

Location privacy has, for national security purposes, little to expect from location technology. As long as the location data is a prerequisite for enabling the communication, the location data will be processed and as such available to security and intelligence agencies if legislation allows them to use these data. In this respect, security and intelligence agencies fully rely on the data that is been process and stored by the telecommunication providers.

One may question whether the European telecommunication providers do not store and process too much detailed data. Strictly reading the EU Directive 2002/58/EC, telecom providers should not be required to provide location data (more than traffic data) if the communication is within a country. The traffic data can even be limited to stating that 'the BTS was in country A', instead of documenting data from a specific BTS. Only in cross-national communications it is necessary to document these detailed data as long as the fees vary from country to country. However, the Data Retention Directive (2006/24/EC) requires to store traffic data. In addition, it may be difficult due to the way the telecom network (technology) currently is designed. Further, providers may want to use the current characteristics to offer location specific discounts (e.g., calling for free in your neighbourhood). An assumed costly change of the network technology and losing a potential marketing instrument are

likely arguments that will withhold telecom providers to introduce a privacy compliant infrastructure.
In addition, for hybrid systems such as using WiFi for VoIP and a mobile device, the WiFi router only needs to know that a mobile device wants to use VoIP. Since VoIP is free there is no need to process the identifiers of the mobile device. In this way, hybrid systems may be not only a big threat to privacy, but also the privacy saviour of the future.

12.5 Technological developments

Developments in technology are expected to result in hybrid systems that incorporate a location identifying component. We foresee developments towards the integration of location information available within WiFi networks, RFID networks, cellphone networks, together with active GPS in mobile devices. Although we might be several years from full integration of these networks, these potentially allow the permanent identification of individuals within a range of a few metres. It is almost impossible not to use devices attached to these networks since we then choose not to participate in modern life. The development of a true privacy enhancing technology that provides the user full control over his devices regarding location information would be the challenge for location technology research. Directions for balancing privacy interests with other interests of society may be found in non-centralised storage of information. Such privacy-preserving directions are, for example, developed for the Transport Information Monitoring Environment (TIME) (Evans et al. 2007).
In addition, hybrid systems such as using WiFi for VoIP and a mobile device, the WiFi router only needs to know that a mobile device wants to use VoIP. Since VoIP is free there is no need to process the identifiers of the mobile device. In this way, hybrid systems may be not only a big threat to privacy, but also the privacy savior of the future.

12.6 International developments

The international developments are tending to develop towards one system of protecting national security. This development include that measures that one countries deemed to be effective and sufficient are now introduced or considered in other countries. That is only measures in addition to the current ones are considered resulting in harmonised legislation at the most intrusive level. For example, the government of Canada (unsuccessfully) proposed to adopt similar legislation as EU on mandatory data retention for communication services. Similarly, the Dutch legislators introduced legislation on data from transportation providers/ carriers, including telecommunication services and airline carriers, with legislation similar to that already existing in Germany. It seems that most 'adopting' take the success of these new measures for granted. Research on the effectiveness of these means is scant, but does not withhold the development towards a worldwide standard of the most intruding level of means available to security and intelligence services. Even if these means appear not to be used at all in the country of origin. Independent scientific research assessing the effectiveness of increased mandates for law enforcement and national security agencies is required. The suggested 3% effectiveness of CCTV in the UK and the 0.01% effectiveness of financial transactions in the Netherlands suggest measures that are disproportional with respect to privacy.

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. Once the law is in place it will be difficult to change or replace it even when the threat has disappeared (see IPTS 2003; Koops 2006, p.36). Developments to the other side, i.e., focused on the protection of privacy, are rare. For example, the introduction of the Canadian Privacy Impact Assessment would be a welcome improvement in European Union member states, but remains unconsidered.

12.7 Less privacy, more security?

Table 12.1 shows a general assessment of the balancing of national security and privacy in the case-studies. Although the table may provide reason to draw several conclusions, it does not imply that the Netherlands is a safer place than Canada. It does, however, confirm the findings of privacy international and EPIC (2007) that privacy protections are significant in Canada and Germany, while modest in the Netherlands.

	Netherlands	Canada	Germany
Privacy protections	-	+	+
Means to protect national security	+	-	+

Table 12.1 A rough indication of the privacy protections and means to protect national security in case-studies relative to each other

Cameron (2007) argues that law enforcement and intelligence services are very well able to combat crime and terrorism, but they will be unable to prevent the root causes of discontent in societies. He further argues that the result of more investigative powers for law enforcement and intelligence services may not be more security and less human rights, but less security and less human rights.

12.8 Summary

Central in this research was the question "How far should the right to privacy reach with respect to the location data from mobile devices used by intelligence and security agencies to protect the national security?" The answer this 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. Therefore, the balancing strongly builds on the balancing process. 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 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 commis-

sion, and information on the number and type of special means by the security and intelligence agency is published.

Opinion of ECtHR judge Pettiti

"The legislation of numerous European States fails to comply with Article 8 of the Convention where telephone tapping is concerned. States use – or abuse – the concepts of official secrets and secrecy in the interests of national security. Where necessary, they distort the meaning and nature of that term. Some clarification of what these concepts mean is needed in order to refine and improve the system for the prevention of terrorism.
The warnings of jurists and parliamentarians go back more than twenty years: the Schmelck Report in France, the advisory opinion I gave to the Luxembourg parliament, the Government White Paper in the United Kingdom and the Court's Klass, Malone, Kruslin and Huvig judgments have all remained largely ineffective. The people running the relevant State services remain deaf to these injunctions and to a certain extent act with impunity. Apart from the specific problem, is this not a sign of the decadence of the democracies; does it not reveal to what extent the meaning of human dignity has been eroded? For this depressing trend States and individuals must share responsibility."

References

Literature

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

Achelpöhler, Wilhelm, and Holger Niehaus (2004). Data Screening as a Means of Preventing Islamist Terrorist Attacks on Germany. *German Law Journal* 5: 495-512.

AIV (Adviescommissie Informatiestromen Veiligheid) (2007). Data Voor Daadkracht; Gegevensbestanden Voor Veiligheid: Observatie En Analyse. 66: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Akerboom, E.S.M. (2003). Contraterrorisme in Nederland.

Albrecht, Hans-Jörg, Claudia Dorsch, and Christiane Krüpe (2003). Rechtswirklichkeit Und Effizienz Der Überwachung Der Telekommunikation Nach Den §§ 100a, 100b Stpo Und Anderer Verdeckter Ermittlungsmaßnahmen. 44: MAX-PLANCK-INSTITUT FÜR AUSLÄNDISCHES UND INTERNATIONALES STRAFRECHT.

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

Arai-Takahashi, Yutaka (2002). *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the Echr*. Antwerp: Intersentia.

Article 19 (1995). The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, Freedom of Expression and Access to Information. U.N. Doc. E/CN.4/1996/39 (1996).

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

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

Barkhuus, Louise, and Anind Dey (2003). Is Context-Aware Computing Taking Control Away from the User? Three Levels of Interactivity Examined. Paper presented at the UBICOMP 2003, 5th International Symposium on Ubiquitous Computing, October 12-15

——— (2003). Location-Based Services for Mobile Telephony: A Study of Users' Privacy Concerns. Paper presented at the Proceedings of Interact 2003, Zurich, Switzerland

Bauer, Laura (2007). Police Find Body of Kansas Kidnapping Victim. *McClatchy Newspapers* 2007.

Belasco, Amy (2003). Total Information Awareness Programs: Funding, Composition, and Oversight Issues. Report for U.S. Congress.

Bellman, Steven, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society* 20: 313–24.

Beresford, Alastair R., and Frank Stajano (2003). Location Privacy in Pervasive Computing. *IEEE Pervasive Computing* 2, no. 1: 46-55.

BKA (Bundeskriminalamt) (2005). Polizeiliche Kriminalstatistik 2005; Bundesrepublik Deutschland.

Blok, Peter (2002). *Het Recht Op Privacy*. Nijmegen: Boom juridische uitgevers.

Boutellier, Hans, Pieter Ippel, and Sima Nieborg (2005). 'Veiligheid Gegarandeerd' En 'Privacy Gered'; Twee Voorstelbare Toekomstbeelden in Nederland Anno 2030. edited by Bureau Strategische Kennisontwikkeling rapport in opdracht van het Ministerie van BZK, 46. Utrecht: Verwey-Jonker instituut.

Breitkreuz, Garry, and Gord Brown (2007). Rights, Limits, Security: A Comprehensive Review of the Anti-Terrorism Act and Related Issues. Report of the Standing Committee Public Safety and National Security; Subcommittee on the Review of the Anti-terrorism Act.

Bundesnetzagentur (2007). Jahresbericht 2007.

Bundestag, Deutscher (2005). Antwort Der Bundesregierung Auf Die Große Anfrage Der Abgeordneten Gisela Piltz, Ernst Burgbacher, Rainer Funke, Weiterer Abgeordneter Und Der Fraktion Der Fdp – Überprüfung Der Personengebundenen Datenschutzrechtlichen Bestimmungen.

Buruma, Ybo (2001). *Buitengewone Opsporingsmethoden*. 2nd ed. Vol. 34, *Studiepockets Strafrecht*. Deventer: W.E.J. Tjeenk Willink.

Cameron, Iain (2007). Different Forms of Oversight in Various Countries. In *Accountability of Intelligence and Security Agencies and Human Rights*, edited by Review Committee on the Intelligence and Security Services (CTIVD) & Faculty of Law Radboud University, 51-60. The Hague.

——— (2000). *National Security and the European Convention on Human Rights*.

Camp, L. Jean, and Carlos Osorio (2002). Privacy-Enhancing Technologies for Internet Commerce. 16: John F. Kennedy School of Government Harvard University Faculty Research Working Papers Series.

Canadian Government (2007). Response of the Government of Canada to the Final Report of the House of Commons Standing Committee on Public Safety and National Security Subcommittee on the Review of the Anti-Terrorism Act; Rights, Limits, Security: A Comprehensive Review of the Anti-Terrorism Act and Related Issues.

CBP (college bescherming persoonsgegevens) (2004). Camera's in Het Publieke Domein. 64: College bescherming persoonsgegevens.

CBP (College bescherming persoonsgegevens) (2007). De Vernietiging Van Geheimhoudersgesprekken; Een Onderzoek Naar De Naleving Van Artikel 126aa Lid 2 Sv Door De Tapkamers in Epe En Driebergen. 52.

CBP (college bescherming persoonsgegevens) (2006). Privacy En De Ov-Chipkaart; De Visie Van Het College Bescherming Persoonsgegevens (Cbp). 2.

Chang, Shuchih Ernest, Ying-Jiun Hsieh, Chien-Wei Chen, Chun-Kuei Liao, and Shiau-Ting Wang (2006). Location-Based Services for Tourism Industry: An Empirical Study. Paper presented at the LNCS 4159

Clarke, R. (2001). Person - Location and Person - Tracking: Technologies, Risks, and Policy Implications *Information Technology & People* 14, no. 2: 206-31.

Clarke, Roger (1994). Dataveillance: Delivering '1984'. In *Framing Technology: Society, Choice and Change*, edited by Green L. & Guinery R. Sydney: Allen & Unwin.

Colbert, Martin (2001). A Diary Study of Rendezvousing: Implications for Position-Aware Computing and Communications for the General Public. Paper presented at the Proceedings of Supporting Group Work, Boulder, Colorado, USA

Coliver, Sandra (1998). Commentary To: The Johannesburg Principles on National Security, Freedom of Expression and Access to Information. *Human Rights Quarterly* 20, no. 1: 12-80.

Commissie Bestuurlijke Evaluatie AIVD (commissie Havermans) (2004). Aivd in Verandering. 320. Den Haag.

Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (2005). Jaarverslag 2004-2005

——— (2006). Toezichtsrapport Ctivd Inzake Het Onderzoek Van De Aivd Naar Het Uitlekken Van Staatsgeheimen (Rapportnr. 10). 17.

Commission Smith (chair David P. Smith) (2007). Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the Anti-Terrorism Act. Special Senate Committee on the Anti-terrorism Act.

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

Coolsaet, Rik, and Teun Van de Voorde (2006). The Evolution of Terrorism in 2005; a Statistical Assessment. 6. Gent, Belgium: Department of Political Science.

Cvrcek, Dan, Marek Kumpost, Vashek Matyas, and George Danezis (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, George, Stephen Lewis, and Ross Anderson (2005). How Much Is Your Privacy Worth? *Fourth Workshop on the Economics of Information Security*

De Jong, Jitske, Marcel Rietdijk, and Yvette Pluijmers (1997). Vastgoed Persoonlijk Benaderd. edited by Ingrid Van den Berg and Aernout Schmidt, 167-264. Alphen aan den Rijn/Diegem: Samsom Bedrijfsinformatie bv.

Dempsey, James X., and David Cole (1999). *Terrorism & the Constitution: Sacrificing Civil Liberties in the Name of National Security*: First Amendment Foundation.

DPWP (Data Protection Working Party Article 29) (2006). Closing Communiqué. Paper presented at the 28TH INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS 2ND & 3RD NOVEMBER 2006

——— (2007). Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and Other Security Authorities.

ECP.NL (2005). Privacyrechtelijke Aspecten Van Rfid. 58: Ministerie van Economische Zaken.

Eras, P. (1998). Rekeningrijden: de gulden middenweg; Smartcard-technologie nog te traag voor langsracende auto's. *Computable*, 13 March.

ESRAB (European Security Research Advisory Board) (2006). Meeting the Challenge: The European Security Research Agenda. 79.

Evans, D. , A.R. Beresford, T. Burbridge, and A. Soppera (2007). Personal Privacy in Transport Middleware and Applications. Paper presented at the EPSRC WINES workshop, University of Warwick, April

Feinberg, J. (1986). *Harm to Self*. Oxford: Oxford University Press.

Filmon, Gary (2007). The Canadian Model of Security Intelligence Review. In *Accountability of Intelligence and Security Agencies and Human Rights*, edited by Review Committee on the Intelligence and Security Services (CTIVD) & Faculty of Law Radboud University, 37-43. The Hague.

Filton, Gary (2007). The Canadian Model of Security Intelligence Review. In *Accountability of Intelligence and Security Agencies and Human Rights*, edited by Review Committee on the Intelligence and Security Services (CTIVD) & Faculty of Law Radboud University, 37-43. The Hague.

Flaherty, David H. (1999). Visions of Privacy: Past, Present, and Future. In *Visions of Privacy: Policy Choices for a Digital Age*, edited by Colin J. Bennett and Rebecca Gran, 19-38. Toronto, Buffalo, London: University of Toronto Press

Frattini, Franco (2007). Accountability of the Intelligence and Security Agencies and Human Rights. In *Accountability of Intelligence and Security Agencies and Human*

Rights, edited by Review Committee on the Intelligence and Secuirty Services (CTIVD) & Faculty of Law Radboud University, 29-33. The Hague.

Fried, Charles (1968). Privacy. *The Yale Law Journal* 77, no. 3: 475-93.

Gabor, Thomas (2004). The Views of Canadian Scholars on the Impact of the Anti-Terrorism Act. University of Ottawa with support from Department of Justice Canada.

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

Goldacre, Ben (2006). How I Stalked My Girlfriend. *The Guardian*, Wednesday February 1, 2006 2006.

Grossklags, Jens, and Alessandro Acquisti (2007). When 25 Cents Is Too Much: An Experiment on Willingness-to-Sell and Willingness-to-Protect Personal Information. Paper presented at the Workshop on the economics of information security (WEIS), Pittsburgh, PA (USA), 7-8 June

Gruteser, Marco, and Dirk Grunwald (2004). A Methodological Assessment of Location Privacy Risks in Wireless Hotspot Networks. *Lecture notes in computer science* 2802: 10-24.

Haggerty, Kevin D., and Richard V. Ericson (2000). The Surveillant Assemblage. *British Journal of Sociology* 51, no. 4: 605-22.

Heise online (2007). Bundesnetzagentur Veröffentlicht Jahresstatistik Zur Telefonüberwachung. 26 April 2007.

——— (2005). Telefonüberwachungen 2004 Wieder Stark Angestiegen. *Heise online*, 31 March 2005 2005.

Henrici, Dirk, and Paul Müller (2004). Tackling Security and Privacy Issues in Radio Frequency Identification Devices. In *Pervasive 2004, Lncs 3001*, edited by A. Ferscha and F. Mattern, 219-24: Springer-Verlag Berlin Heidelberg.

Hutcheon, Stephen (2006). Satellite Snaps Topless Sunbathers. *The Sunday Morning Herald*, September 27, 2006 2006.

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).

IVIR (Institute for Information Law) (2005). Dutch Constitution Translated.

Jacoby, Nicole (2006). The Decision of the Bundesverfassungsgericht of April 12, 2005 – Concerning Police Use of Global Position Systems as a Surveillance Tool. *The German Law Journal*.

——— (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, no. 7: 1085-92.

——— (2006). Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States. *bepress Legal Series*.

JupiterResearch (2007). Location-Based Services: Where Are You? *Cited by GPS Businessnews available at: http://www.gpsbusinessnews.com* 2007.

Kaasinen, E. (2005). User Acceptance of Location-Aware Mobile Guides Based on Seven Field Studies. *Behaviour & Information Technology* 24, no. 1: 37-49.

Kamerstukken 2006-2007 nr. 31145: (proposed) Implementation Act of the Data retention Directive 2006/24/EU (Wetsvoorstel bewaarplicht telecommunicatiegegevens).

Kamerstukken 2006-2007 nr. 31145 nr. 3; Explanatory Memorandum of the (proposed) Implementation Act of the Data retention Directive 2006/24/EU (Wetsvoorstel bewaarplicht telecommunicatiegegevens).

Kamerstukken 2005-2006, nr. 29876 nr. 18; Evaluatie AIVD; Lijst van vragen en antwoorden over de uitspraak in het kort geding dat door de Telegraaf tegen de Staat der Nederlanden is aangespannen

Kamerstukken 2004-2005 nr. 29441 E (Eerste Kamer); Wijziging Wetboek van Strafvordering en enkele andere wetten in verband met bevoegdheden tot het vorderen van gegevens.

Kamerstukken 2003-2004, nr. 29441, nr. 3; Wijziging Wetboek van Strafvordering en enkele andere wetten in verband met bevoegdheden tot het vorderen van gegevens; memorie van toelichting.

Kamerstukken 2002-2003, aanhangsel van de handelingen 1553 under 1

Kamerstukken 2002-2003, aanhangsel van de handelingen 1035

Kamerstukken 2001–2002, nr. 28059, nr. 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 2000-2001 27591 nr. 2; Grootschalig afluisteren van moderne telecommunicatiesystemen; Lijst van vragen en antwoorden

Kamerstukken 1998-99, 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*).

Kamerstukken 1997-1998, nr. 25533, nr., 8, p.11; Parliamentary discussion Telecommunication Act

Kamerstukken 1996-97 nr. 25403 nr. 3; Explanatory Memorandum

Kamerstukken 1994-1995, nr. 22036 nr. 6; Verwijdering en vernietiging dossiers Binnenlandse Veiligheidsdienst; Brief minister met nota over uitspraken van de Raad van State over inzage van BVD-dossiers

Kamerstukken nr. 29413; Wijziging Beginselenwet justitiële jeugdinrichtingen

Kamerstukken nr. 25877; Parliamentary discussion Act on the Intelligence and Security Services 2002 (*Behandeling van de WIV 2002*).

Kamerstukken 1997-1998, nr. 25877 nr. 3; Explanatory Memorandum Act on the Intelligence and Security Services 2002.

Karimi, H. A., and A. Hammad (2004). *Telegeoinformatics: Location-Based Computing and Services*: Taylor & Francis.

Kohnstamm, Jacob, Lynsey Dubbeld, and Hanneke Schmeets (2007). Nederland Controlestaat; Ook Eerlijke Burgers, Die Niets Te Verbergen Hebben, Moeten Zich Zorgen Maken over Aantasting Van Hun Privacy. *Trouw*, 30 June 2007.

Koops, B.J. (2006). *Tendensen in Opsporing En Technologie; over Twee Honden En Een Kalf*. Nijmegen: Wolf Legal Publishers.

Koops, B.J., and Ronald Leenes (2005). 'Code' and the Slow Erosion of Privacy. *Michigan Telecommunications and Technology Law Review* 12, no. 1: 115-88.

Koops, B.J., and A.H. Vedder (2001). Opsporing Versus Privacy: De Beleving Van Burgers. In *ITeR-reeks*, 124. Den Haag: Sdu Uitgevers.

Korff, Douwe (2002). Ec Study on Implementation of Data Protection Directive Comparative Summary of National Laws. . Cambridge (UK).

Krumm, John (2007). A Survey of Computational Location Privacy. Paper presented at the WORKSHOP ON UBICOMP PRIVACY, Innsbruck, Austria, September 16

Lamer, Antonio (2005). Submission [of Communications Security Establishment (Cse) Commissioner] to Justice Dennis O'connor, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar.

Lee, Gunhee, Wonil Kim, and Dong-kyoo Kim (2005). An Effective Method for Location Privacy in Ubiquitous Computing. *LNCS (EUC Workshops 2005)* 3823: 1006-15.

Leeuwarder Courant (2008). Onderzoek Naar Foto's Vliegbasis. *Leeuwarder Courant* 2008, 7 januari.

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. New York Basic Books.

Levi, Michael, and David S. Wall (2004). Technologies, Security, and Privacy in the Post-9/11 European Information Society. *Journal of Law and Society* 31, no. 2: 194-220.

Lips, A.M.B., S. van der Hof, J.E.J. Prins, and A.A.P. Schudelaro (2004). Issues of on-Line Personalisation in Commercial and Public Service Delivery. Tilburg: University of Tilburg.

Lo, A. (2007). Mobile and Wireless Networks, Slides Ae4-E07. Delft, 2007.

Lockton, Vance, and Richard S. Rosenberg (2006). Rfid: The Next Serious Threat to Privacy. *Ethics and Information Technology (2005)* 7: 221-31.

Logtenberg, Hugo (2008). Brother Wordt Steeds Bigger; De Overheid Ziet Alles - En Wij Vinden Het Best? *Intermediair* 18 januari 2008, no. 3: 16-21.

Longley, Paul A., Michael F. Goodchild, David J. Maguire, and David W. Rhind (2001). *Geographic Information Systems and Science*. Chicester, England: John Wiley and Sons Ltd.

Loof, J.P. (2005). *Mensenrechten En Staatsveiligheid: Verenigbare Grootheden?* Nijmegen: Wolf Legal Publishers.

——— (2006). Noot 89. *European Human Rights Cases (EHRC)* 7, no. 7: 818-33.

Louis Harris & Associates, and A.F. Westin (1994). [Unpublished Survey Report].

Luccio, Matteo (2007). Sirf and Skyhook Develop Hybrid Gps-Wifi Positioning System. *GIS Monitor*, February 8 2007.

——— (2006). Skyhook Wireless Launches Wireless Position System. *GIS Monitor*, 6 April 2006.

Ludford, Pamela J., Dan Frankowski, Ken Reily, Kurt Wilms, and Loren Terveen (2006). Because I Carry My Cell Phone Anyway: Functional Location-Based Reminder Applications. 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, April 22–27

Mahnken, Eva (2005). Mindestspeicherungsfristen Für Telekommunikationsverbindungsdaten; Rechtstatsachen Zum Beleg Der Defizitären Rechtslage. Bundeskriminalamt.

Margulis, Stephen T. (2003). On the Status and Contributions of Westin's and Altman's Theories of Privacy. *Journal of Social Issues* 59, no. 2: 411-29.

——— (2003). Privacy as a Social Issue and a Behavioral Concept. *Journal of Social Issues* 59, no. 2: 243-61.

Marx, Gary T. (1998). Ethics for the New Surveillance. *The Information Society* 14: 171-85.

——— (2003). A Track in the Shoe: Neutralizing and Resisting the New Surveillance. *Journal of Social Issues* 59, no. 2: 369-90.

——— (2002). What's New About The "New Surveillance"? Classifying for Change and Continuity. *Surveillance and Society* 1, no. 1: 9-29.

Matyas, Vashek, and Marek Kumpost (2007). Location Privacy Pricing and Motivation. Paper presented at the The 8th International Conference on Mobile Data Management (MDM'07) Workshop Proceedings (The International

Workshop on Privacy-Aware Location-based Mobile Services (PALMS 07)), Mannheim, Germany

McCullagh, Declan (2006). Fbi Taps Cell Phone Mic as Eavesdropping Tool. *CNET News*, December 4 2006.

McSmith, Andy (2008). The Big Question: Are Cctv Cameras a Waste of Money in the Fight against Crime? *The Independent*, 7 May.

Mell, Patricia (1996). Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the

Electronic Wilderness. *Berkeley Technology Law Journal* 11: 11-92.

Mevis (Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij) (2001). Gegevensvergaring in Strafvordering; Nieuwe Bevoegdheden Tot Het Vorderen Van Gegevens Ten Behoeve Van Strafvorderlijk Onderzoek.

Miedema, Frank, and Bob Post (2006). Evaluatie Pilot Elektronische Volgsystemen. 63. 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.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2007). Strategie Nationale Veiligheid.

Mokbel, Mohamed F. (2007). Privacy in Location-Based Services: State-of-the-Art Abd Research Directions. Paper presented at the presentation at PALMS workshop Mannheim

Mul, V., P.C. Verloop, J.H.J. Verbaan, and M.C. Bannier (2005). Wie Bewaart Die Heeft Wat; Onderzoek Naar Nut En Noodzaak Van Een Bewaarverplichting Voor Historische Verkeersgegevens Van Telecommunicatieverkeer.

Myjer, Egbert (2007). How Can Human Rights Best Be Guaranteed? In *Accountability of Intelligence and Security Agencies and Human Rights*, edited by Review Committee on the Intelligence and Secuirty Services (CTIVD) & Faculty of Law Radboud University, 45-50. The Hague.

Neve, Rudie, Lisette Vervoorn, Frans Leeuw, and Stefan Bogaerts (2006). Eerste Inventarisatie Van Contraterrorismebeleid: Duitsland, Frankrijk, Italië, Spanje, Het Verenigd Koninkrijk En De Verenigde Staten - 'Research in Progress'. WODC in opdracht van de NCTb.

Nouwt, Sjaak, Berend R. de Vries, and Corien Prins (2004). *Reasonable Expectations of Privacy?*, *Information Technology & Law Series*: T.M.R. Asser Press.

O'Conner, Dennis (2006). A New Review Mechanism for the Rcmp's National Security Activities; Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar.

O'Harrow Jr., Robert (2005). *No Place to Hide; Behind the Scenes of Our Emerging Surveillance Society*. New York: The Free Press.

Odell, Mark (2005). Use of Mobile Helped Police Keep Tabs on Suspect and Brother. *Financial Times*, August 2 2005.

Onsrud, H.J. , J. Johnson, and X. Lopez (1994). Protecting Personal Privacy in Using Geographic Information Systems. *Photogrammetric Engineering and Remote Sensing* LX, no. 9: 1083-95.

Palen, Leysia, and Paul Dourish (2003). Unpacking "Privacy" for a Networked World. Paper presented at the CHI 2003, Ft. Lauderdale, Florida, USA., April 5-10

Pedersen, D.M. (1999). Model for Types of Privacy by Privacy Functions. *Journal of Environmental Psychology* 19, no. 4: 397-405.

Peissl, Walter (2002). Surveillance and Security a Dodgy Relationship. In *Debating Privacy and Ict - before and after September 11*, edited by D. van Harten: Rathenau instituut.

Penders, Jacques (2004). Privacy in (Mobile) Telecommunications Services. *Ethics and Information Technology* 6: 247-60.

Pincus, Walter, and Dan Eggen (2006). 325,000 Names on Terrorism List. *Washingtonpost.com*, Wednesday, February 15, 2006; A01 2006.

Ponce, Phil (1999). The Wrong Target PBS online newshour.

PriceWaterhouseCoopers (2003). A&K Analyse Op Een Vijftal Interceptie Organisaties En -Systemen.

Prins, Corien (2000). Privacy, Consument En Het Recht Op Anonimiteit: Een Oud Fenomeen in Een Nieuw Jasje In *De E-Consument. Consumenten-Bescherming in De Nieuwe Economie*, edited by NVvIR-studiecommissie 'ICT en consument'.

——— (2006). Property and Privacy: European Perspectives and the Commodification of Our Identity (Chapter X). In *The Future of the Public Domain*, edited by L. Guibault and P.B. Hugenholtz, 223-57. The Netherlands: Kluwer Law International.

Privacy international, and EPIC (Electronic Privacy Information Center) (2007). The 2007 International Privacy Ranking.

Questiaux, Nicole (1982). Study of the Implications for Human Rights of Recent Developments Concerning Situations Known as States of Siege or Emergency. UN sub-commission on Prevention of Discrimination and Protection of Minorities.

Raab, Charles D., and Colin J. Bennett (1998). The Distribution of Privacy Risks: Who Needs Protection? *The Information Society* 14: 263-74.

Raad van Hoofdcommissarissen (commissie Welten) (2004). Spelverdeler in De Opsporing; Een Visie Op Forensische Opsporing. 48. Amsterdam: Projectgroep Forensische Opsporing.

Rachels, James (1975). Why Privacy Is Important. *Philosophy and. Public Affairs* 4: 323-33.

RAND Corporation (2004). Mapping the Risks; Assessing the Homeland Security Implications of Publicly Available Geospatial Information. 237: Prepared for the National Geospatial-Intelligence Agency.

Raper, Jonathan (2002). Brave New World? *GeoEurope*.

Ravi (Raad voor Vastgoedinformatie) (1992). Structuurschets Vastgoedinformatievoorziening Delen I, Ii En Iii,. edited by Apeldoorn 1992.

Regan, Priscilla M. (2002). Privacy and Commercial Use of Personal Data: Policy Developments in the United States. In *Debating Privacy and Ict - before and after September 11*, edited by D. van Harten, 33-46: Rathenau instituut.

Registratiekamer (1996). Credit Scoring Database.

Reijne, Z., R.F. Kouwenberg, and M. P. Keizer (1996). Tappen in Nederland. Arnhem: WODC/ Gouda Quint.

Ringelestijn, Tonie van (2006). Voor Het Eerst Cijfers Internettaps Openbaar. *Netkwesties*, 17 oktober 2006 2006.

ROB (Raad voor het openbaar bestuur) (2005). Tussen Oorlog En Vrede; Kader Voor Een Balans Tussen Vrijheidsrechten En Veiligheid. 74.

Roberts, Adam (2002). Can We Define Terrorism? *Oxford today* 14, no. 2.

Rogers, Everett M. (1993). The Diffusion of Innovations Model. In *Diffusion and Use of Geographic Information Technologies*, edited by I. Masser and H.J. Onsrud, 9-24. Dordrecht, the Netherlands: Kluwer Academic Publishers.

Ross (2005). Germany's Federal Constitutional Court and the Regulation of Gps Surveillance. *The German Law Journal* , 6, no. 12: 1805-12.

Rotenberg, Marc, Cédric Laurant, Ula Galster, and Katitza Rodríguez Pereda (2006). 2006 International Privacy Survey; an International Survey of Privacy Laws and Developments. Washington D.C./ London: Electronic Privacy Information Center and Privacy International

Rotenberg, Marc, and Allison Knight (2004). Privacy and Human Rights 2004. EPIC and Privacy International.

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

Schmid, G. (Tijdelijke Commissie Echelon-interceptiesysteem) (2001). Ontwerpverslag over Het Bestaan Van Een Wereldwijd Systeem Voor De Interceptie Van Particuliere En Economische Communicatie (Echelon-Interceptiesysteem). 112.

Sciannamea, Michael (2004). Companies Increasingly Use Gps-Enabled Cell Phones to Track Employees. *thewifiweblog*, Sep 24th.

Scourias, John (1997). Overview of the Global System for Mobile Communications.

Sietsma, Ruben (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

SIRC (Security Intelligence Review Committe) (2006). SIRC Annual Report 2005-2006; an Operational Review of the Canadian Security Intelligence Service.

——— (2007). SIRC Annual Report 2006-2007; an Operational Review of the Canadian Security Intelligence Service.

Smith, Jessica, and Allison Kealy (2003). SDI and Location Based Wireless Applications. In *Developing Spatial Data Infrastructures: From Concept to Reality*, edited by Ian Williamson, Abbas Rajabifard and Mary-Ellen F. Feeney, 263-79. London: Taylor and Francis.

Snow, John (1855). On the Mode of Communication of Cholera. London: John Churchill, New Burlington Street, England.

Spiekermann, S. , J. Grossklags, and B. Berendt (2001). E-Privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behaviour. Paper presented at the ACM Electronic Commerce 2001 Conference

Staal, Herman (2008). Alleen Aandacht Voor Radicalen; Ontwikkelaar Zwicht Voor Bedreigingen: Zeldzaam Succes Voor Dierenactivisten. *NRC Next*, 8 Januari 2008, 10-11.

Stokmans, Derk (2007). Ik Heb Niks Te Verbergen; Nederlanders Zijn Naief. Ze Weten Niet Wat De Overheid Allemaal Mag. *nrc.next*, 23 mei 2007, 5.

Stratix (2003). Onderzoek "Bewaren verkeersgegevens door telecommunicatieaanbieders". 89: Eindrapport Uitgebracht aan het Wetenschappelijk Onderzoeken Documentatiecentrum van het Ministerie van Justitie.

Taylor, H. (2003). Most People Are Privacy Pragmatists, Who, While Concerned About Privacy, Will Sometimes Trade It Off for Other Benefits. *The Harris Poll*, March 19 2003, 17.

The Special Senate Committee on the Subject Matter of Bill C-36 (2001). First Report.

Thompson, Clive (2007). The Visible Man: An Fbi Target Puts His Whole Life Online. 15, no. 06.

Tokmetzis, Dimitri (2007). Altijd Loert Het Wakend Oog; Technologie En Juridische Bevoegdheden Zijn Een Gevaar Voor De Privacy in Nederland. *NRC Handelsblad*, 12 mei 2007, 41.

Tomesen, Remco (2007). Adverteerders Ontdekken Bluetooth. *Emerce*, 28 maart 2007 2007.

Trubow, G.B. (1990). Protecting Informational Privacy in the Information Society. *Northern*
Illinois University Law Review 10: 521-42.
van der Bel, D., A.M. van Hoorn, and J.J.T.M. Pieters (2007). *Informatie En Opsporing; Handboek Informatieverwerving, -Verwerking En - Verstrekking Ten Behoeve Van De Opsporingspraktijk*, *Ssr-Publicaties*. Zeist: Uitgeverij Kerckebosch.
van der Geest, Thea , Willem Pieterson, and Peter de Vries (2005). Informed Consent to Address Trust, Control, and Privacy Concerns in User Profiling. Paper presented at the Proceedings of the UM2005 conference Edinburg , Scotland
van de Pol, Wim (2006). *Onder de tap; afluisteren in Nederland*. Amsterdam: Uitgeverij Balans.
van Hulst, Sybrand J. (2007). Independent Review of Intelligence and Security Services: A View from the Aivd. In *Accountability of Intelligence and Security Agencies and Human Rights*, edited by Review Committee on the Intelligence and Secuirty Services (CTIVD) & Faculty of Law Radboud University, 75-80. The Hague.
van Loenen, Bastiaan (2006). *Developing Geographic Information Infrastructures; the Role of Information Policies*. Dissertation, Delft: DUP Science.
Van Wijngaarden, W. (2001). Niet-Satelliet Gebaseerde Locatietechnieken En - Diensten. *Technieuws*.
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.
——— (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.
——— (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.
——— (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.
Venice commission (European commission for democracy through law) (2007). Report on the Democratic Oversight of the Security Services.
Verdonck, Klosster & Associates bv (2006). Onderzoek Naar De Nationale Implementatie Van De Europese Richtlijn Dataretentie. Ministerie van Justitie.
Verhue, Dieter (2007). Nationaal Vrijheidsonderzoek - Opiniedeel Meting 2007. Amsterdam: Veldkamp.
Verhue, Dieter, Dick Verzeijden, and Annet Nienhuis (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.
Verhue, Dieter, Dick Verzijden, and Annet Nienhuis (2006). Nationaal Vrijheidsonderzoek - Opiniedeel Meting 2006; Een Onderzoek Naar Opinie, Kennis En Draagvlak Ten Aanzien Van 4 En 5 Mei. Amsterdam: Veldkamp.
Walker, Karyl (2007). Dispute over Digital Maps Stalls Electronic Monitoring System for Convicts. *Jamaica Observer*.
Walters, Gregory J. (2001). Privacy and Security. *ACM SIGCAS Computers and Society* 31, no. 2: 8-23.
Warren, Samuel D., and Louis D. Brandeis (1890). The Right to Privacy. *Harvard Law Review* IV, no. 5: 193-220.

Westin, Alan F. (1967). *Privacy and Freedom*. New York: Atheneum.
——— (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues* 59, no. 2: 431-53.
Wheeler, Brian (2004). This Goes No Further... *BBC News Online Magazine*, March 2 2004.
White, James C. (2003). People, Not Places; a Policy Framework for Analyzing Location Privacy Issues. Masters, Duke University
Whitman, James Q. (2004). The Two Western Cultures of Privacy: Dignity Versus Liberty. *The Yale Law Journal* 113: 1151-221.
Wood, David Murakami, and Kirstie Ball (2006). A Report on the Surveillance Society for the Information Commissioner, by the Surveillance Studies Network.
Young, Jason (2007). Constitutional Rights and New Technologies in Canada. In *Constitutional Rights and New Technologies; a Comparative Study Covering Belgium, Canada, France, Germany, Sweden, and the United States*, edited by Bert-Jaap Koops, Ronald Leenes and Paul De Hert, 43-67. Tilburg: TILT – Tilburg Institute for Law, Technology, and Society.
Zimmer, M. (2006). Surveillance, Privacy and the Ethics of Vehicle Safety Communication Technologies. *Ethics and Information Technology* 7: 201-10.
Zöller, Verena (2004). Liberty Dies by Inches: German Counter-Terrorism Measures and Human Rights. *The German Law Journal* 5, no. 5: 469-94.
Zwaap, René (2007). Duitse Pers Afgeluisterd. *PM Europa* 1, no. 21: 4.

Websites

Website	Web address
AIVD	https://www.aivd.nl/taken/aandachtsgebieden
BfV	http://www.verfassungsschutz.de/en/en_about_bfv/tasks.html
Bundestag	http://www.bundestag.de/parlament/gremien/kontrollgremien/parlkon/mitglieder.html
CSEC	http://www.csec-ccst.gc.ca/mandate/index_e.php
CSIS	http://www.csis-scrs.gc.ca/en/priorities/terrorism.asp
CSIS	http://www.csis-scrs.gc.ca/en/about_us/intelligence.asp
CTIVD	http://www.ctivd.nl/leden.html
CTIVD	http://www.ctivd.nl/?English
DPWP	http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.
GILC	http://www.gilc.org/privacy/survey/intro.html
Globalstar	http://www.globalstar.info/globalstar_services.html
IEEE	http://www.ieee-virtual-museum.org/collection/tech.php?id=2345893&lid=1
livecontacts	http://www.livecontacts.com/
Marketing-facts	http://www.marketingfacts.nl/berichten/20060912_verboden_plekken_in_nederland/
mediatheek	http://mediatheek.thinkquest.nl/~kla039/index.php?site=gen2&
Ministry of Justice	http://www.justice.gc.ca/en/anti_terr/rep_res/cc_hc/rep_res_annex.html
MIVD	http://www.mindef.nl/binaries/mivd_nl_tcm15-27995.pdf)
Nu	http://www.nu.nl/news/824632/50/Noordwijk_wil_van_Google-vlek_af.html
OECD Ottawa	http://www.ottawaoecdconference.org/))
OHCHR	http://www.ohchr.org/english/bodies/hrc/index.htm
OHCHR 2	http://www.ohchr.org/english/about/publications/docs/fs2.htm#universal
OHCHR 3	http://www.ohchr.org/english/about/publications/docs/fs2.htm#worldwide
Privacy Council Office	http://www.pco-bcp.gc.ca/default.asp?Language=E&Page=informationresources&Sub=publications&Doc=role/role2007_e.htm#3
REI	http://www.rei.com/product/758168
Silicon	http://www.silicon.com/research/specialreports/protectingid/0,3800002220,39121670,00.htm
SIM	http://sim.law.uu.nl/SIM/Library/books.nsf/a1c506a79c314718c125668200337d46/1dae41371892327ac125664000368491?OpenDocument
SIRC	http://www.sirc-csars.gc.ca/rvwetd/index-eng.html
Space	http://www.space.com/businesstechnology/technology/satellite_phones_030321.html

UN	http://www.un.org/aboutun/charter/
University of Minnesota	http://www1.umn.edu/humanrts/gencomm/hrcom16.htm
US Coast Guard	http://www.navcen.uscg.gov/marcomms/ais.htm
Vorratsdaten-speicherung	http://www.vorratsdatenspeicherung.de/
Vorratsdaten-speicherung 2	http://www.vorratsdatenspeicherung.de/content/view/176/55/lang,de/

Appendix Case law

European Court of Human Rights judgments

- Amann: Amann v. Switzerland (Application no. 27798/95); 16 February 2000
- Belgian Linguistic Case (Application nº 1474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64) 23 July 1968
- Dudgeon: Dudgeon v. the United Kingdom, (application no. 7525/76), 22 October 1981
- Erdem: Erdem v. Germany, Application no. 38321/97, 5 July 2001
- Halford: Halford v. the United Kingdom, (application no. 73/1996/692/884), 25 June 1997, Reports of Judgments and Decisions 1997-III, p. 1017
- Handyside: Handyside v. The United Kingdom, (Application no. 5493/72); 7 December 1976
- Hatton: Case of Hatton and Others v. UK (No.1), (application no. 36022/97 2003), 2 October 2001
- Herbecq: Herbecq and the Association "Ligue des droits de l'homme" v. Belgium, applications nos. 32200/96 and 32201/96, Commission decision of 14 January 1998, DR 92-B
- Huvig: Huvig v. France (Application no. 11105/84); 24 April 1990
- Kahn: Kahn v. United Kingdom (Application no. 35394/97) 4 October 2000
- Klass: Klass and Others v. Germany, (application no. 5029/71), 6 September 1978
- Kopp: Kopp v. Switzerland (13/1997/797/1000); 25 March 1998
- Kroon: Kroon and others v. The Netherlands, Application no. 18535/91
- Leander: Leander v. Sweden (application no. 9248/81), 26 March 1987
- Malone: Malone v. United Kingdom, (application no. 8691/79), 2 August 1984
- Marckx: Marckx v. Belgium, (application no. 6833/74), 13 June 1979
- Niemietz: Niemietz v. Germany (Application no. 13710/88); 16 December 1992
- Norris: Norris v. Ireland judgment, (application no. 10581/83),
- Olsson: Olsson v. Sweden (No.1), (application no. 10465/83), 24 March 1988
- P.G. and J.H.: P.G. and J.H. v. The United Kingdom (Application no. 44787/98); 25 September 2001, FINAL judgment: 25/12/2001
- Padro Bugallo: Prado Bugallo v. Spain, (Application no 58496/00); 18 February 2003, final 18/05/2003
- Peck: Peck v. UK, (appl. no. 44647/98), 28 April 2003
- Refah Partisi: Refah Partisi (the welfare party) and others v. Turkey (applications nos. 41340/98, 41342/98, 41343/98 and 41344/98) judgment Strasbourg 31 July 2001
- Rotaru: Rotaru v. Romania, (application number 28341/95), 4 May 2000
- Segerstedt: Segerstedt-Wiberg and others v. Sweden, (appl. no. 62332/00), 6 June 2006
- Silver: Silver And Others v. The United Kingdom, (Application no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75); 25 March 1983
- Sunday Times: Sunday Times v. The United Kingdom (No. 2) (Application no. 13166/87); 26 November 1991

- Surek: Sürek v. Turkey (no. 3), (application no. 24735/94), 8 July 1999
- Valenzuela Contreras: Valenzuela Contreras v. Spain (58/1997/842/1048); 30 July 1998
- Weber: Weber and Savaria v. Germany, (appl. no. 54934/00), 29 June 2006

Judgments from the European Court of Human Rights are available through: http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/

Dutch case law referred to

- Valkenier (R01.91.0306)
- Court of Appeal in The Hague 25 January 2000 LJN AE0196
- Court Arnhem 30 July 2004 LJN AQ5858
- HR 5 June 2007 LJN BA1024;
- Court of Appeal in The Hague 29 June 2004 LJN AQ1112
- Court Haarlem LJN AX9578
- Court Maastricht LJN AZ8384
- Court of Appeal in The Hague LJN AQ1112
- HR 21 March 2000 LJN AA5254
- HR 19 March 1997
- HR 9 January 1987
- HR 19 February 1991
- HR 12 February 2002 LJN AD9222
- HR 2 June 1998
- HR NJ 1995, 684
- HR 12 February 2002 LJN AD9222
- Van Baggum: afd. bestuursrechtspraak Raad van State 16 juni 1994, AB 1995, 238 (nrs. R01.91.1588)
- HR 19 December 1995; Zwolsman-arrest; zaaknummer 101269, NJ 1996/249
- HR 17 September 2002 LJN AE4200
- HR 10 December 2002 LJN AE9632
- HR 7 September 2004 LJN AO9090
- Court Amsterdam 20 April 2006 LJN AW2513

Cases are available through http://www.rechtspraak.nl

Canadian Case law referred to

- BMG v. John Doe, (F.C.), (2004) FC 488 http://www.canlii.org/en/ca/fct/doc/2004/2004fc488/2004fc488.html
- BMG v. John Doe; Written testimony of Shaw Communications Inc. http://www.cippic.ca/documents/file-sharing-lawsuits/document-archives.html
- Federal Court (1997): Canadian Security Intelligence Service Act (Re) (T.D.) 1997 CanLII 6377 (F.C.) http://www.canlii.org/en/ca/fct/doc/1997/1997canlii6377/1997canlii6377.html
- 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
- R. v. Collins, (1987) 1 S.C.R. 265, http://csc.lexum.umontreal.ca/en/1987/1987rcs1-265/1987rcs1-265.pdf
- R. v. Duarte (1990) 1 S.C.R. 30, http://scc.lexum.umontreal.ca/en/1990/1990rcs1-30/1990rcs1-30.pdf
- R. v. Edwards (1996) 1996 CanLII 255 (S.C.C.) http://www.canlii.org/en/ca/scc/doc/1996/1996canlii255/1996canlii255.html
- R. v. Plant (1993) CanLII 70 (S.C.C.) http://www.canlii.org/en/ca/scc/doc/1993/1993canlii70/1993canlii70.html
- R. v. Tessling (2004) 3 S.C.R. 432, SCC 67, http://scc.lexum.umontreal.ca/en/2004/2004scc67/2004scc67.pdf
- R. v. Thompson, (1990) CanLII 43 (S.C.C.), http://www.canlii.org/en/ca/scc/doc/1990/1990canlii43/1990canlii43.html
- R. v. Weir, (1998) A.J. No. 155; [2001] A.J. No. 869
- R. v. Wise (1992) 1 S.C.R. 527, http://scc.lexum.umontreal.ca/en/1992/1992rcs1-527/1992rcs1-527.pdf
- R. v. Wong, (1990) 3 S.C.R. 36, CanLII 56 (S.C.C.) http://www.canlii.org/en/ca/scc/doc/1990/1990canlii56/1990canlii56.html

Canadian Charter: http://laws.justice.gc.ca/en/charter/#libertes

German case law referred to

- *Census Act Case* (*Volkszählung* (Census)) (1983); BVerfGE 65, 1.
- *Lauschangriff Case* (2004) BVerfG, 1 BvR 2378/98 from March 3, 2004, available at http://www.bverfg.de/entscheidungen/rs20040303_1bvr237898.html
- Federal Constitutional Court, BVerfG, 1 BvR 2226/94 of 07/14/1999, available at: http://www.bundesverfassungsgericht.de/entscheidungen/rs19990714_1bvr222694.html (German) or http://www.bundesverfassungsgericht.de/entscheidungen/rs19990714_1bvr222694en.html (English)
- *GPS Case* (2005), 25 BVerfG, 2 BvR 581/01 from April 12, *available at* http://www.bverfg.de/entscheidungen/rs20050412_2bvr058101.html
- *Rasterfahndung* case (2006), 1 BvR 518/02 of 4 April 2006, available at: http://www.bverfg.de/entscheidungen/rs20060404_1bvr051802.html
- *Datenschutzes im Telekommunikationsrecht* case (2006), BVerfG, 1 BvR 1811/99, 27.10.2006, available at: http://www.bverfg.de/entscheidungen/rk20061027_1bvr181199.html

United States case law

- 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

Appendix interviewees

Netherlands

Hans Pieters
Lector strafrecht, Training and Study Centre for the Judiciary

Jan Rijnders
Senior Consultant KPN Security

Ybo Buruma
Hoogleraar Straf- en strafprocesrecht, Radboud Universiteit Nijmegen

Jan Peter Loof
Universitair docent Staats- en Bestuursrecht, Universiteit Leiden

John de Bekker
Korps landelijke politiediensten (KLPD); Dienst Specialistische Recherche Toepassingen

Frans van Eenbergen
Beleidsadviseur Arrondissementsparket 's-Hertogenbosch; Stafbureau bovenregionaal rechercheoverleg

Astrid Buijs
Parketvoorlichter Arrondissementsparket 's-Hertogenbosch

Canada

Christopher Pounce
Strategic Policy Analyst, Office of the Privacy Commissioner of Canada

Tim Farr
Associate Executive Director, Security Intelligence Review Committee

Jason M. Young
Barrister & Solicitor, Toronto Canada

Germany

Johann Eckers
Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BFDI)

Michael vom Hagen
Pressereferat – Bundesamt fuer Verfassungsschutz

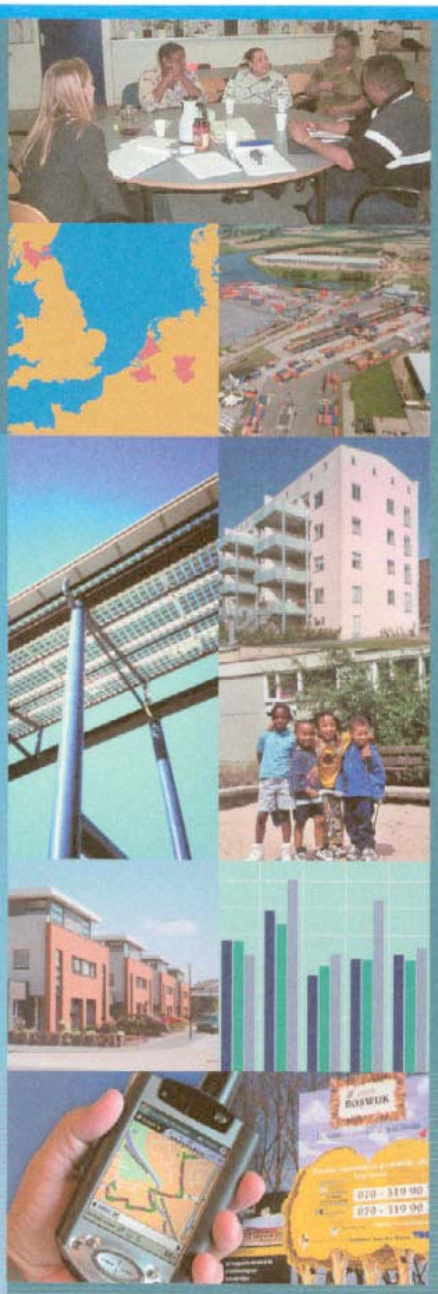
Hans-Jörg Albrecht
Director at the Max Planck Institute for Foreign and International Criminal Law in Freiburg/Germany (MPI)

Appendix glossary of acronyms

AIVD	Algemene Inlichtingen- en Veiligheidsdienst	Dutch Intelligence and Security Agency
AuC	Authentication Center	
BfV	Bundesamt für Verfassungsschutz	German Federal Office for the Protection of the Constitution
BND	Bundesnachrichtendienst	German Federal Intelligence Service
BSC	Base Station Controller (BSC).	A BSC manages the connection between one or more BTSs
BTS	Base Transceiver Stations	telecommunication towers
BverfSchG	Bundesverfassungsschutzgesetz	Act Regulating the Cooperation between the Federation and the Federal States in matters relating to the Protection of the Constitution and the Federal Office for the Protection of the Constitution of Germany
CCTV	Closed Circuit TV	
Convention 108	Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data	
CSES	Communications Security Establishment (Canada)	
CSIS	Canadian Security and Intelligence Agency	
ECHR	(European) Convention for the Protection of Human Rights and Fundamental Freedoms	
ECtHR	European Court of Human Rights	
EIR	Equipment Identity Register	
EPC	Electronic Product Codes'	"Streepjescodes"
ESRAB	European Security Research Advisory Board	An in April 2005 formed board of 50 high-level specialists and strategists and 5 members of the European parliament and 14 members of the European Commission, to make a significant contribution towards addressing security research and technology needs.
GLONASS	Global Navigation Satellite System	Russian navigation system

GPS	Global Positioning System	US navigation system
GSM	Global System for Mobile communications	Also acronym for cellphone
HLR	Home Location Register	
ICCPR	International Covenant on Civil and Political Rights	
IMEI	International Mobile Equipment Identity	identity of the cellphone
IMSI	International Mobile Subscriber Identity	identity of the SIM card
IRNSS	Indian Regional Navigational Satellite System	Indian navigation system (planned)
MAD	Militärischer Abschirmdienst	German Military Security and intelligence service
MSC	Mobile Services Switching Centre	
MSISDN	International Mobile Subscriber Identity	'phone number' of the cellphone
OECD	Organisation for Economic Co-operation and Development	The OECD groups 30 member countries (primarily countries with a high socio-economic level of development) sharing a commitment to democratic government and the market economy.
PDA	Personal Data Assistant	
PET	Privacy enhancing technology	
PIPEDA	Personal Information Protection and Electronic Documents Act	Canada's privacy law for private sector processing of personal information
PIT	Privacy invading technology	
PKG	*Parlamentarische Kontrollgremium*	parliamentary Supervisory Board on Intelligence and Security Agencies
PKGrG	Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Kontrollgremiumgesetz -	Act Regulating parliamentarian Control over the Intelligence and Security Agencies (in Germany)
RCMP	Royal Canadian Mounted Police	
RFID	Radio Frequency Identification technology	
UWB	Ultra wideband	
VLR	Visitor Location Register	
Wbp	Wet bescherming persoonsgegevens	Dutch Data Protection Act
WIFI	Wireless Fidelity	
WLAN	Wireless local area networks	
WPAN	wireless personal area network	

WPS	Wireless Positioning Systems	
XPS	Ubiquitous positioning system	Positioning system integrating GPS and WPS



**OTB Research Institute for Housing,
Urban and Mobility Studies
Delft University of Technology
Jaffalaan 9, 2628 BX Delft, The Netherlands
Postbus 5030, 2600 GA Delft, The Netherlands
Telefoon +31 (0)15 278 30 05
Fax +31 (0)15 278 44 22
E-mail mailbox@otb.tudelft.nl
www.otb.tudelft.nl**