

Location privacy and national security: contradiction in terminus?

Bastiaan VAN LOENEN
Delft University of Technology,
OTB Research institute for the Built Environment,
the Netherlands,
b.vanloenen@tudelft.nl

Abstract

Location based services (LBS) potentially put the privacy of individuals at risk. The increased possibility to know people's whereabouts is posing the question of possibility versus desirability with regard to location privacy. The central question that this article aims to answer is how location privacy needs of cell phone users may be balanced with national security needs of society? Through a study of literature and rulings of the European Court of Human Rights a balancing framework was developed. The framework allowed for the assessment of the situation in the Netherlands, Germany and Canada with respect to the location data from mobile devices used by intelligence and security agencies to protect the national security. The research shows that the balancing should account for the totality of the circumstances. 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. A proper balancing strongly builds on the balancing process, especially when balancing is very context-sensitive. This process should be just with adequate safeguards against abuse.

Keywords: Location privacy; National security; Mobile devices

1 Introduction

Location based services (LBS) are among these relatively new ICT developments that potentially put the privacy of individuals at risk. LBS technology allows for tracking and tracing the location of mobile phones or other terminal equipment. These are widely available and becoming increasingly precise in defining a location, opening new possibilities for government and commercial use of location information. Information about people's whereabouts, especially in combination with existing location information about a person (see De Jong et al., 1997), may reveal detailed information about personal profiles, relationships, and other aspects of personal life.

This paper addresses location privacy in the context of national security. The central question that this paper aims to answer is how may location privacy needs of cell phone users be balanced with national security needs of society? Special attention was provided to the rulings of the European Court of Human Rights on the balancing of privacy and national security interests.

A case study was used to apply a balancing framework to the existing balancing practices in three countries: the Netherlands, Germany and Canada. These were performed through literature studies on the current legislation, and court rulings on privacy and national

security. Confirmation with the findings was sought through interviews with knowledgeable experts.

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

2 Privacy

Most people would affirm the importance of privacy. However, the sense of what must be kept private differs from person to person. Privacy means different things to different people (Westin, 2003, p.442). Some people love to give away their full personal life in TV shows or YouTube, while others are very reserved in providing their phone number or address. Penders (2004, p.253) has explained this behaviour in the confidentiality of spheres. Within one sphere, for example the medical sphere, the work sphere, or private home sphere, data can be exchanged and in certain instances one expects that data is exchanged; e.g., the doctor exchanges your personal file with the hospital. However, many would object against exchanging personal data between spheres. For example, your doctor exchanging your medical file with your supervisor.

However, contexts may change and impact attitudes towards privacy (see Westin, 1967, 2003, p.433; Margulis, 2003; Koops and Leenes, 2005, p. 149).

2.1 Location privacy

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

The linkage of information to the earth makes the object or subject easy to identify, and as a result easy to reach, and/ or to determine the relative position between two devices. With data about a person's past and present locations, it is possible to impute aspects of the person's (future) behaviour.

2.2 Context of the location information

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

interfere with the daily life of the individual (see also Gruteser and Grunwald, 2004, p.13). Linking location information to a 'sensitive' context will imply that the location information also should be treated as sensitive information.

2.3 Timeliness of location information

Time may have similar characteristics as location. The knowledge of what one is doing now may be considered private today. But twenty years from now, this information might be irrelevant. In this respect, Cvrcek et al. (2006) found that location data of mobile phones extracted in the first month seems to be most valuable: "An observer gets a lot of information at the start of an observation period, such as their usual moving pattern. Subsequent months add very little information, and can therefore be seen as less valuable both from the point of the observer, and the person observed". This holds of course until the observed individual shows unusual behavioural patterns.

Generally, real-time location information is likely to be considered more sensitive than one's location in the past. In specific instances, however, this general guideline may not apply. For example, if old location data is linked to a specific expectation (e.g., at work), and it appeared that this expectation was falsified (e.g., with a mistress), the location information might be personal information.

2.4 Use mode: active, passive, or no use

Also the use mode of a mobile device may influence the extent to which the right to privacy is interfered with. We distinguished three types of use-modes: active use (e.g., calling), passive use (stand-by) and no use (device is turned off). The active use mode includes communicating with another device or individual. The user is aware that he is communicating with others. He even may be aware that his communications may be noticed by others. This is less likely for passive use. Mobile telephones in the standby mode may send transmissions to the local tower, enabling to track a person's movements (Clarke, 2001, p.213; see also Gruteser and Grunwald, 2004, p.15). 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). Thus even if the cell-phone is in the standby mode, it may still be tracked down to a location (see *US v. Forest*). The more active the use, the less infringing the interference with the right to privacy may be.

3 National security

The concept of national security is difficult to define because it is closely related to subjective and sometimes emotional perceptions of administrations and military authorities about the threats to national security (Loof, 2005, p.235; see also Roberts, 2002). National security aims to protect a nation from internal and external factors threatening the continued existence of the norms that are the fundament of today's society. Therefore, a (democratic) constitutional state has the right to defend itself against intrusions on its (territorial) integrity including intrusions from other states, or against intrusions of the order of law within a state (Loof, 2005, p.105; see also Explanatory

report of Convention 108). National security may be defined as the universal process of surveillance by authorities to enforce the rules and taboos of society (cf. Marx 2002, p.20; Westin, 1967, p.20; UN Economic and Social Council *Siracusa Principles*).

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

Technology allowing surveillance, such as location technology, is increasingly important to protect 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). 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). Location information of mobile devices may also be useful for law enforcement or security and intelligence services; who was where at the time of the crime, where did he go, with whom and where is the suspect now (see, for example, Data Retention Directive 2006/24/EC, recital 11). Further, it can be used to identify the risk-posing individuals and their networks (Mul et al., 2005, p.26). It is also important in verifying the statements or testimonies of victims, suspects, witnesses (Mul et al., 2005, p.26), or to assess or confirm the reliability of an informant, although the legitimacy of such action is disputed in the literature. 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.

4 Balancing framework of the European Court of Human Rights in its rulings

The right to privacy is in most international treaties recognised as a fundamental human right. The right is, however, not absolute. National security interests can justify a limitation to the right to privacy. However, states may not, in the name of protecting national security, adopt whatever measures they deem appropriate. As a practical fact, absolute privacy is difficult to accomplish, but absolute security may be as problematic to reach (see AIV, 2006, p.8). What is the proper balance between national security and privacy? (O'Harrow Jr., 2005, p.13; Westin, 1967; Levi and Wall, 2004). The (European) Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) is at the core of European privacy legislation. It addresses privacy in article 8:

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

The ECtHR's rulings on article 8 ECHR further specified and explained article 8. It 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).

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

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

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

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

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

Starting point in this section is that there is a need to address national security threats. Question is then what means to use, for how long, among others. Special focus is on the use of telecommunication data with respect to principles 2 and 3.

5 Applying the principles: case study results

5.1 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).

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.

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

According to the ECtHR's settled case law, a legitimate aim needs to be pursued, and there should be a "reasonable relationship of proportionality between the means employed and the aim sought to be realised" (*Marckx* §33, *Dudgeon* §53). If the aim sought can be realised with alternative less intrusive means, the ECtHR finds the intrusion disproportionate (*Olsson* §83, *Hatton* §97). This principle is also known as the subsidiary principle.

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

5.2.1 Effective use of location data

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

Data from cell-phones are not by definition reliable law enforcement means, however. Some suspects use this knowledge to give their cell-phone to their husband on the day of a robbery and use another (prepaid) cell-phone. This cell-phone may then be destroyed directly after the robbery. The location data of a beacon only provides the location of the object – and not necessarily also of the subject – on which the beacon was placed. Location data of a cell-phone provides some evidence of the presence of a device at a certain location at a certain time. However, it is not necessarily the nearest telecommunication tower that is being used in the communications. It may very well be a tower several kilometres away from the location of the cell-phone. In addition, in the Netherlands, only traffic data is stored. Thus, only the tower used at the start of a communication and the tower that is used at the moment of ending the communication are stored. The telecommunication towers used in between are not stored. Therefore, fully depending on the location data of a cell-phone for preventing a crime or for solving crimes is insufficient.

5.2.2 Subsidiary criterion: assessing an order of privacy interfering means

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

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

5.2.3 Proportionality

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.

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 (PIA) may be used to assess the privacy impact of several selected effective means. Canadian federal agencies are required to perform a privacy impact assessment for proposals for programs and services that raise privacy risks (Lemieux, 2007).

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

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

5.3.1 Balancing of telecommunication data use: data from the case-studies

Each country in the case study has a different regime for information related to or concerning location. In the Netherlands, no independent authority is involved in the decision to use special authorities by the intelligence and security agency. Only if the operations involve the content of communications, the Minister has to approve use of the measure. In Canada no distinction is made in the law between any type of information. Although the Federal Court might be likely to easier accept or require lower standards for requests concerning solely identification data compared to the full range of available telecommunications data, this was not confirmed in this research. Depending on the totality of the circumstances of a case, a greater or lesser reasonable expectation of privacy may be found. The expectation of privacy in private areas, i.e., the home, is

greater than in public areas. In Germany, the decision model is most detailed developed in the law. The independent G-10 commission needs to approve the surveillance of traffic data and location data of mobile devices, putting these at the same level as the content of communications.

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

The detailed legislation in Europe may ignore the totality of the circumstances in the decision to use a special means such as a wiretap, or real-time tracking of an individual. This categorisation in law assumes that the right to privacy is a rather absolute concept which can be applied in the same manner, whatever the specific circumstances of a case may be. However, real-time location information may sometimes be considered very privacy sensitive information, while the content of a nonsense conversation with a family member may not. In addition, in some instances it is very sensitive information with whom you communicated, no matter what was discussed or where it was discussed. These nuances may not be part of the decision-making procedure to use special means like wiretapping, or claiming location information. At least, they are not necessarily acknowledged in the hierarchy of the approval structure.

5.3.2 Effectiveness of means and subsidiarity in case studies

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

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

Concerning the effectiveness of means, we may take the number of phone taps as an example to compare differences of used means between case study countries. These

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

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

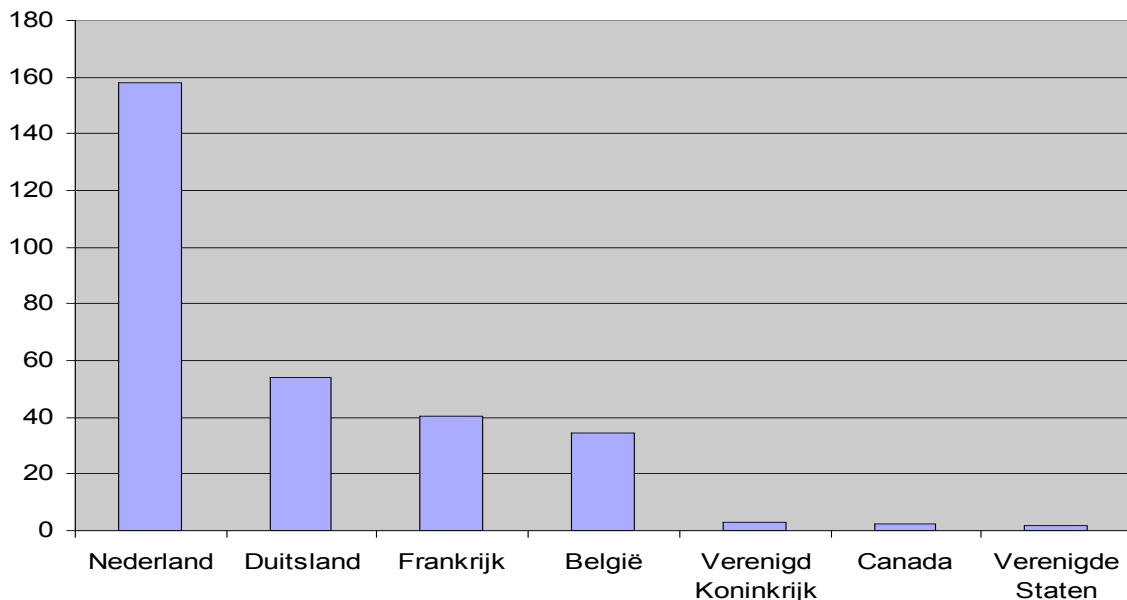


Figure 1: The approximate number of taps for law enforcement in the case-study countries per 100 000 citizens

6 Conclusion

How far the right to privacy should reach with respect to the location data from mobile devices used by intelligence and security agencies to protect the national security depends on the totality of the circumstances. 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, proper balancing builds on the balancing process, especially when balancing is context-sensitive. This process should be just with adequate safeguards against abuse.

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

Contrary to the transparency requirement of the European Court of Human Rights this research suggests that law describing the available means to protect national security in general terms will better respect the right to privacy than legislation describing in great details when to use what means. Additional research is required to evidence this hypothesis further.

Acknowledgements

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

References

- AIV (Adviescommissie Informatiestromen Veiligheid), 2007. Data voor daadkracht; Gegevensbestanden voor veiligheid: observatie en analyse. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.
- Allen, A., 1988. *Uneasy Access: Privacy for Women in a Free Society*. Rowman and Littlefield, Totowa, N.J.
- Altman, I., 1975. *The Environment and Social Behavior*. Brooks/ Cole Publishing Company, Monterey, California.
- Beresford, A.R., & Stajano, F., 2003. Location Privacy in Pervasive Computing. *IEEE Pervasive Computing*, 2(1), 46-55.
- Bundesnetzagentur, 2007. *Jahresbericht 2007*.
- Buruma, Y., 2001. *Buitengewone opsporingsmethoden* (2nd ed., Vol. 34). W.E.J. Tjeenk Willink, Deventer.
- Clarke, R., 2001. Person - Location and Person - Tracking: Technologies, Risks, and Policy Implications *Information Technology & People*, 14(2), 206-231.
- Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention no. 108)
- Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms* (ECHR)
- Cvrcek, D., Marek Kumpost, Vashek Matyas, & Danezis, G. 2006. *A Study on The Value of Location Privacy*. a study undertaken in the framework activities around the FIDIS Network of Excellence presented at WPES 2006.
- De Jong, J., Rietdijk, M., & Pluijmers, Y., 1997. Vastgoed persoonlijk benaderd. in: I. Van den Berg & A. Schmidt (Eds.), *Samsom Bedrijfsinformatie bv*, Alphen aan den Rijn/Diegem, pp. 167-264.

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 (1995).
- Directive 2002/58/EC of The European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
- Directive 2006/24/EC of The European Parliament and of The Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
- DPWP (Data Protection Working Party Article 29), 2006. CLOSING COMMUNIQUÉ. Paper presented at the 28th International Conference of Data Protection and Privacy Commissioners.
- Dudgeon*: *Dudgeon v. the United Kingdom*, (application no. 7525/76), 22 October 1981, European Court of Human Rights judgment (see <http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/>)
- EC Regulations No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.
- Gruteser, M., & Grunwald, D., 2004. A methodological assessment of location privacy risks in wireless hotspot networks. Lecture notes in computer science, 2802, 10-24.
- Hatton*: *Case of Hatton and Others v. UK (No.1)*, (application no. 36022/97 2003), 2 October 2001, European Court of Human Rights judgment (see <http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/>)
- 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).
- Koops, B.J., & Leenes, R., 2005. 'Code' and the Slow Erosion of Privacy. Michigan Telecommunications and Technology Law Review, 12(1), 115-188.
- Leander*: *Leander v. Sweden* (application no. 9248/81), 26 March 1987, European Court of Human Rights judgment (see <http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/>)
- Lemieux, D., 2007. Privacy Impact Assessment from a Regulator's Point of View. Paper presented at the Privacy Horizons: Terra Incognita (29th International Conference of Data Protection and Privacy Commissioners).
- Levi, M., & Wall, D.S., 2004. Technologies, security, and privacy in the post-9/11 European information society. Journal of Law and Society, 31(2), 194-220.
- Longley, P.A., Goodchild, M.F., Maguire, D.J., & Rhind, D.W., 2001. Geographic information Systems and Science. John Wiley and Sons Ltd, Chicester, England.
- Loof, J.P., 2005. Mensenrechten en staatsveiligheid: verenigbare grootheden? Wolf Legal Publishers, Nijmegen.

- Marckx*: Marckx v. Belgium, (application no. 6833/74), 13 June 1979, European Court of Human Rights judgment (see <http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/>)
- Margulis, S.T., 2003. Privacy as a social issue and a behavioral concept. *Journal of Social Issues*, 59(2), 243-261.
- Marx, G.T., 2002. What's new about the "new surveillance"? Classifying for change and continuity. *Surveillance and Society*, 1(1), 9-29.
- McCullagh, D., 2006. FBI taps cell phone mic as eavesdropping tool. *CNET News*, December 4.
- Minister of Justice, 2008. Tapstatistieken, Brief aan de Voorzitter van de Tweede Kamer der Staten-Generaal, 27 mei.
- Minister of Public Safety Canada, 2007. Annual report on the use of electronic surveillance 2006.
- Mul, V., Verloop, P.C., Verbaan, J.H.J., & Bannier, M.C., 2005. Wie bewaart die heeft wat; Onderzoek naar nut en noodzaak van een bewaarverplichting voor historische verkeersgegevens van telecommunicatieverkeer.
- Myjer, E., 2007. How can human rights best be guaranteed? in: Review Committee on the Intelligence and Security Services (CTIVD) & Faculty of Law Radboud University (Ed.), *Accountability of Intelligence and Security Agencies and Human Rights* (The Hague, pp. 45-50.
- Nouwt, S., de Vries, B.R., & Prins, C., 2004. *Reasonable Expectations of Privacy?* T.M.R. Asser Press.
- O'Harrow Jr., R., 2005. *No place to hide; Behind the scenes of our emerging surveillance society*. The Free Press, New York.
- Olsson*: Olsson v. Sweden (No.1), (application no. 10465/83), 24 March 1988, European Court of Human Rights judgment (see <http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/>)
- Penders, J., 2004. Privacy in (mobile) telecommunications services. *Ethics and Information Technology*, 6, 247-260.
- R. v. Plant* (1993) CanLII 70 (S.C.C.), Canada, available at: <http://www.canlii.org/en/ca/scc/doc/1993/1993canlii70/1993canlii70.html>
- Roberts, A., 2002. Can we define terrorism? *Oxford today*, 14(2).
- Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights, Annex, UN Doc E/CN.4/1984/4 (1984). United Nations, Economic and Social Council, U.N. Sub-Commission on Prevention of Discrimination and Protection of Minorities(1984).
- US. v. Tomero* (2006): SD New York, USA v. John Tomero Et Al., No. S2 06 Crim. 0008 (LAK)
- van de Pol, W., 2006. *Onder de tap; afluisteren in Nederland*. Uitgeverij Balans, Amsterdam.
- van Loenen, B., & Zevenbergen, J.A., 2007. The impact of the European privacy regime on location technology development. *Journal of Location Based Services*, 1(3), 165-178.
- Walters, G.J., 2001. Privacy and security. *ACM SIGCAS Computers and Society*, 31(2), 8-23.

- Warren, S.D. & Brandeis, L.D., 1890. The right to privacy. *Harvard Law Review*, IV(5), 193-220.
- Weber*: Weber and Savaria v. Germany, (appl. no. 54934/00), 29 June 2006, European Court of Human Rights judgment (see <http://www.echr.coe.int/ECHR/EN/Header/Case-Law/HUDOC/HUDOC+database/>)
- Westin, A.F., 1967. *Privacy and Freedom*. Atheneum, New York.
- Westin, A.F., 2003. Social and political dimensions of privacy. *Journal of Social Issues*, 59(2), 431-453.
- Wong, F.-L., & Stajano, F., 2005. Location Privacy in Bluetooth. in: R. Molva, G. Tsudik & D. Westhoff (Eds.), *ESAS 2005*, LNCS 3813, pp. 176-188.