SDIs and Privacy: Conflicting Interests of the Spatially Enabled Society[1]

Bastiaan van Loenen & Jitske de Jong, Delft University of Technology

Introduction

The availability of information in information societies is a key issue that affects the entire society's well-being. The possibilities for discovering new insights about the natural world, which have both commercial and public interest value, are extraordinary (NRC 1999a, p. 34).

Developments in information technology have improved significantly the level of detail, currency of the data, but above all their interoperability. It is currently possible to link a wide variety of data sets at any time, and independent from their and your geographic location. Interoperable geographic data sets are at the core of SDI concepts.

However, for the highest level of geographic detail, when the data can be linked to individuals, the ever-increasing level of interoperability poses serious threats to privacy rights. At these detailed levels the interest of a society for the concept of SDI may conflict with privacy interests of that same society.

SDIs in advanced stages of development are expected to be driven by value added services (see Van Loenen 2006). Among the most promising value added services are location based services. However, especially for these services, privacy concerns may be a serious threat to the success and further development of LBS. This chapter explores the SDI (development) with respect to privacy considerations.

SDI & society

Spatial data infrastructures concentrate on information integration, reducing duplication, using resources more effectively, and creating a base from which to expand industry productivity and the geographic information market (Rajabifard et al., 2003, pp. 101, 107; Rajabifard et al., 2002b, p. 14). Although the "information focus" is typically for the first generation SDIs, the linking of geographic data sets is key to the success of SDI. An appropriate definition of a GII is: a framework continuously facilitating the eficient and effective generation, dissemination, and use of needed geographic information within a community or between communities (after Kelley, 1993).

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 geographic and administrative data is concerned. The information infrastructure will at least bring us what we already have, but in ways that are better, faster and cheaper (King and Kraemer, 1995, p. 14). It will promote economic development and make countries highly competitive.

[1] Published as: Van Loenen, B. and de Jong, J. 2007, 'SDIs and Privacy: Conflicting Interests of the Spatially Enabled Society', Chapter 21, In A. Rajabifard (ed.), *Towards a Spatially Enabled Society*, ISBN 978-0-7325-1620-8, University of Melbourne, pp. 271-284.

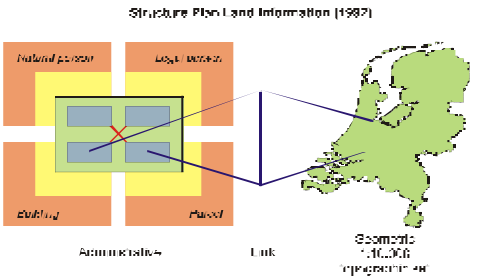

Figure 1: SDI optimised: ubiquitous linking of framework data sets (Ravi, 1992)

At certain levels of positional accuracy, location information identifies individuals. At these levels location information is also considered personal information. In the Netherlands this level of accuracy has been set below the 6 digit zip-code level (6PPC). Other counties may have different interpretations of the personal information definition of the European privacy Directive 95/46/EC provisions (see Korff 2002).

It is foreseen that "as society becomes more technically savvy, spatially aware and more demanding of services available through mobile devices, more detailed and more enhanced services are likely to be required" (Smith and Kealy, 2003). They envision a GII that could promote "Location Based Services development through the provision of high quality spatial data" (Smith and Kealy, 2003). The recent value-added services of GoogleEarth/maps 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).

Privacy & society

Frequently, privacy is described as the right to be let alone (after Cooley 1880). More comprehensively, Margulis (2003, p.415) found that "many definitions of privacy appear to share a common core of key elements: Privacy involves control over transactions (interactions, communications) that regulate access to self and that as a consequence, reduce vulnerability and increase decisional and behavioral options." This, also, involves when [personal information] will be obtained and what uses will be made of it by others (see Westin 1967).

Westin (1967, 13) has argued that privacy norms may vary among societies, but the functions of privacy remain the same. "Privacy provides opportunities for self-assessment and experimentation. It is a basis for the development of individuality. It protects personal autonomy. It supports healthy functioning 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. In sum, privacy is important because it is posited to provide experiences that support normal psychological functioning, stable interpersonal relationships, and personal development." (Margulis 2003, 246, citing Westin 1967).

"Westin also posits four specific functions (purposes, the whys) of privacy:

- "Personal autonomy: the desire to avoid being manipulated, dominated, or exposed by others.
- Emotional release: refers to release from the tensions of social life.
- Self-evaluation: refers to integrating experience into meaningful patterns and exerting individuality on events.
- Limited and protected communication: limited communication sets interpersonal boundaries; protected communication provides for sharing personal information with trusted others."

(Margulis 2003)

In line with these ethical notions the desire for privacy protection has lead to legislation in several jurisdictions. It has also been the subject of provisions lead down in international legislation. Privacy is one of the fundamental rights as being recognized by international law, such as the UN Universal

Declaration of Human Rights (art. 12) and the European Convention for the protection of Human rights and Fundamental Freedoms..Art. 8 of the Convention reads:
(1) Everyone has the right to respect for his private and family life, his home and his correspondence, and
(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 interest of national security, public safety or the economic well-being of the country, for ( ).

In recent decades international and national legislation protecting the privacy of individuals typically provides the means to individuals to limit the use of their personal information. The OECD rules for data protection and Convention nr 108 Council of Europe are examples of such legislation (see further).

Location privacy
Location information links "place, time, and attributes. Some attributes are physical or environmental in nature, while others are social or economic" (Longley 2001, pp.64-65). The linkage of information to the earth makes the object or subject easy to identify, and as a result easy to reach.

Location information may impose a serious threat to the privacy of the individual that is linked to a place on earth, for example, through the location of his mobile device. The device may frequently be found 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). Conclusions drawn from this information can interfere with the daily life of the individual (see also Gruteser and Grunwald, 2004). This is especially annoying if the conclusions are inaccurate because the found 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 cigars. This may result in unfavorable situations for one's health insurance, for example.
Linking this location tracking and tracing information with other data (address, social security number, income, etc) may reveal a pattern which may contribute to a person's profile.

Within a geographic context, privacy limitation 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.

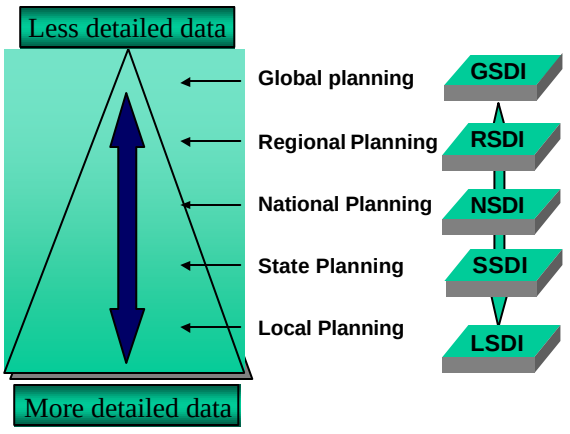

Figure 2: high-level of detail at local levels of SDI (Source based on Rajabifard et al., 1999)

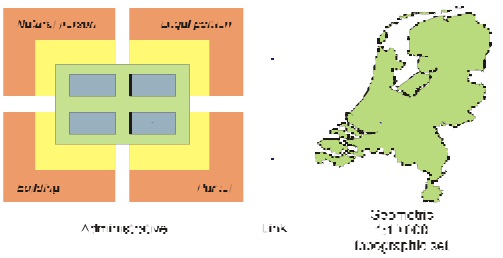

Figure 3: privacy optimised: no linking between datasets (figure based Ravi, 1992)

SDI versus privacy

Opportunities of technology for SDI
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. 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).
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 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. Thus, location technology potentially allows for the ubiquitous surveillance of objects including individuals.
The level of interoperability increases everyday serving many users well.

Technology threatening privacy
The utilization of location technology to its full extent poses serious privacy considerations. Increased interoperability may lead to a society of ubiquitous real-time surveillance of individuals: at all times it is known where one is, what he does and with whom.
Due to technological developments, an increasing amount of administrative and geographical information is available through an increasing number of channels. 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. However, currently it is at least in theory possible to link any data set with any other.
Together, the acquired data allows for inferred assumptions about individual's income, health, lifestyle, buying habits, travel behaviour, and social network, amongst others. Developments in artificial intelligence (see O'Harrow Jr., 2005, 265), the 'individual' becomes more transparent than ever before. Especially, when we want to link public sector data collected for one purpose with private sector data collected for another, and integrate that in a third data set with again another goal, privacy issues are foremost in secondary uses of personal data (cf. O'Harrow Jr. 2005, 291).
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).

Privacy enhancing regulations and technologies: a threat to SDI's?

Privacy regulations
The interoperability of data sets including the continuous tracking of individuals and consequently the further development of the appealing technologies may be blocked by privacy regulations.
Lack of privacy protection would allow the provision of datasets that are commercially attractive (see Ravi bedrijvenplatform, 2000, p. 24), but interfere with the privacy of individuals. Moreover, sometimes government agencies create datasets for specific public purposes. If these records are subject to freedom of information legislation, then the personal information in these datasets need to be subtracted to fulfill requirements of privacy legislation. This value subtracting may be a costly operation, resulting in expensive information creation, and potentially fewer users.

Privacy enhancing technologies
For those that cannot do without the temptations of the information society may use *privacy enhancing technologies (PET)* to avoid surveillance. Anonymisers and encryption are typical PETs. "New technologies have been developed that permit individuals who enter the field of the camera to remain anonymous. Only a court order can then switch off this filter" (IPTS 2003, 103).
For mobile devices one may use an information diffusion approach to scatter the user's location information to confuse the attacker (Lee et al. 2005, 1007), or use frequently changing pseudonyms (Wong et al. 2005, 83). Use of encrypted and anonymously purchased mobile phone communications between offenders make both them and their content difficult to trace (IPTS 2003, 180).
However, there are no guarantees that encrypted or anonymised 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, 213; see also Gruteser et al. 2004, 15, Lee et al. 2005, 1009).
Thus, relying on technology alone to protect individual's privacy may be insufficient. A more comprehensive view on privacy protection and the use of personal data within an SDI is needed.

Privacy in Europe
As mentioned before in Europe, the right to privacy finds its legal basis in the (European) Convention for the Protection of Human Rights and Fundamental Freedoms (article 8). Also the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention no. 108) requires contracting parties to implement the principles set forth by this Convention.
The purpose of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention no. 108) is "to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")" (article 1 Convention 108). The focus is on the processing of personal data. Article 5 of Convention no. 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"

(article 5 Convention 108).

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 that 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.
Although Treaty 108 may be considered not very influential "with regard to the right to private life of Article 8 ECHR" (IPTS 2003, 123), because "[] the Strasbourg Court and Commission have paid very little attention to 'their own' Council of Europe's Treaty 108" (IPTS 2003, 123), its' principles are also

found in the EU Directives governing data protection (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, and 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).

Conclusion

Privacy and SDI interests are potentially conflicting. If personal data is processed according to data management guidelines as required in European legislation, the needs may not conflict.
However, not all countries in the world do have such a comprehensive privacy framework available. In these instances, but also in Europe, it is recommended to involve privacy concerns in discussions on implementing the SDI concept. SDI and privacy can only go hand in hand if the data management is adequately organised. Convention 108 may be used as a basis managing this balance between SDI and privacy interests.

Acknowledgments

This paper has been written to honor Ian Williamson, who will become 60 and at this occasion will step down as Head of the Department of Geomatics, University of Melbourne, Australia. The section on geo-information and land development, of Delft University of Technology has been able to work with Prof. Williamson at various occasions over several years. We admire his achievements and dedication in teaching and research, in particular in the field of Spatial Data Infrastructures, His enthusiasm gave us inspiration to also explore the intriguing aspects of SDI's. Fortunately as a staff-member he will continue to dedicate his work power to the University and the SDI-world-community at large. We wish him all the best.

Jitske de Jong and Bastiaan van Loenen

Literature

T. O. Chan, M.-E. Feeney, A. Rajabifard, and I. Williamson, "The Dynamic Nature of Spatial Data Infrastructures: A Method of Descriptive Classification," *GEOMATICA*, vol. 55, pp. 65-72, 2001.

R. Clarke, "Introducing PITs and PETs: Technologies Affecting Privacy," Privacy Law & Policy Reporter, vol. 7, pp. 181-183,188, 2001.

Cooley T.: Cooley on Torts 2d ed., p. 29. (1880)

M. Gruteser and D. Grunwald, "A methodological assessment of location privacy risks in wireless hotspot networks," Lecture notes in computer science, vol. 2802, pp. 10-24, 2004.

IPTS (Institute for Prospective Technological Studies): 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), (2003)

P. C. Kelley, "A National Spatial Information Infrastructure," presented at Proceedings of the 1993 Conference of the Australasian Urban and Regional Information Systems Association (AURISA), Adelaide, South Australia, Australia, 1993.

J. L. King and K. L. Kraemer, "Information infrastructure, national policy, and global competitiveness," *Information Infrastructure and Policy*, vol. 4, pp. 5-28, 1995.

D. Korff, "EC Study On Implementation of Data Protection Directive Comparative Summary of National Laws.," Cambridge (UK) Study Contract ETD/2001/B5-3001/A/49) September 2002, 2002.

Lee, Gunhee, Wonil Kim and Dong-kyoo Kim, (2005) An effective method for location privacy in ubiquitous computing, In: T. Enokido et al. (ed.) EUC Workshops 2005, Lecture notes in computer science 3823, pp. 1006-1015

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

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

NRC (National Research Council), *Trust in Cyberspace*. Washington, D.C: National Academy Press, 1999a.

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

W. Peissl, "Surveillance and security a dodgy relationship," in *Debating privacy and ICT - before and after September 11*, D. v. Harten, Ed.: Rathenau instituut, 2002.

A. Rajabifard, T. O. Chan, and I. P. Williamson, "The Nature of Regional Spatial Data Infrastructures," presented at AURISA 99 – The 27 th Annual Conference of AURISA Fairmont Resort, Blue Mountains NSW, 1999

Rajabifard, A., M.-E. F. Feeney, and I. P. Williamson, "Directions for the Future of SDI development," *International Journal of Applied Earth Observation and Geoinformation*, vol. 4, pp. 11-22, 2002b.

Rajabifard, A., M.-E. F. Feeney, I. P. Williamson, and I. Masser, "National SDI Initiatives," in *Developing Spatial Data Infrastructures: From Concept to Reality*, I. Williamson, A. Rajabifard, and M.-E. F. Feeney, Eds. London: Taylor and Francis, 2003, pp. 95-110.

Ravi (Raad voor Vastgoedinformatie), 1992, Structuurschets vastgoedinformatievoorziening delen I, II en III, RAVI-rapport nr. 29.

Ravi Bedrijvenplatform, "Economische effecten van laagdrempelige beschikbaarstelling van overheidsinformatie," vol. Ravi publicatie 00-02, 2000, pp. 48.

Rogers, E.M., 1993, The diffusion of innovations model, in: Masser, I. and H.J. Onsrud, Diffusion and Use of Geographic Information Technologies, Dordrecht, the Netherlands (Kluwer Academic Publishers), pp. 9-24.

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

Van Loenen, Bastiaan, 2006, *Developing geographic information infrastructures; the role of information policies.* Dissertation. Delft University of Technology. Delft: DUP Science. http://www.library.tudelft.nl/ws/a/resources_guide/tudelftpublicaties/

Wong, Ford-Long and Frank Stajano, (2005) Location privacy in Bluetooth, In: R. Molva, G. Tsudik and D. Westhoff (eds.) ESAS, Lecture notes in computer science 3813, pp.176-188