

# Network tourism: a fallacy of location privacy!

By Gonçalo Jorge Morais da Costa, Nuno Sotero Alves Silva and Piotr Pawlak

## Abstract

This contribution aims to discuss if “locational” privacy in tourism is a fallacy! Nevertheless, the authors inform that the reason for this debate is 21<sup>st</sup> century tourist distinctive characteristic, constantly “wired” through ICT, leading to serious ethical issues as regards to personal privacy. Therefore, this paper is divided into five core sections: background (tourist, and ICT for tourism and tourist); control (etymology, the thin bound concerning security, and control and personal data); privacy (the concept, evolution, and dimensions); empirical evidences (overview, crime scene investigation, and keen exhibits); and finally, discussion (act 1 and act 2).

## Introduction

Travel and mobility are prominent features of contemporary society and economy, which is justified by 924 million tourist arrivals in 2008 (World Tourism Organization, 2009), being these tourists important consumers of services, including information services, and demonstrating tourism tendency toward IT (Staab and Werthner, 2002). Moreover, preliminary reports of the World Tourism Organization claim that despite the financial crisis in 2008 tourism has grown 6%, which 2009 figures seem to contradict (World Tourism Organization, 2009). Even so, the estimates for 2010 are roughly one billion international arrivals. Therefore, as global trend tourism engages a key role in economics, representing in 2007 over 745 billion dollars (World Travel and Tourism Council, 2007).

However, the aim of this contribution is not to promulgate an extensive outlook regarding the economic performance of tourism, but to question if “locational” privacy in tourism is a fallacy? The praxis for this debate is a consequence of three interactive analytical dimensions: the optimization of travelling experiences by tourism agents, so that tourists avoid unwanted experiences (Kansa and Wilde, 2008); “wired” tourists that require constant available information for daily leisure activities, as well as to identify socially significant locations (Eagle and Pentland, 2006); and, tourists societal control (Nelson, 2009). From the trade-off between new approaches to capture and analyze tourist’s mobility (Wolf, 2004), societal control for security reasons (Mesjasz, 2004), as well as tourists informational needs, it is possible to conclude that within the inner core of this quandary are privacy issues.

## Background

### Tourist

According to 19<sup>th</sup> century historical records, “tourist” was predominantly used in an English context, referring to *those who went to England!* Nonetheless, the classical definition of travelling and recreation has been extended in order to include business and other purposes (Oxford English Dictionary, 2008). Moreover, tourists are typically interested (among other things) in the destinations climate, culture, or its nature.

Despite the previous definition, 21<sup>st</sup> century tourist involves a distinguishing characteristic: it is always “wired” to the surrounding world (network tourism) through multiple ICT platforms (mobile phones, wireless networks, GPS, location-based services, etc.), leading to the concept of virtual tourist. According to Carlvik and Jonsson (2001: 273) “it is a group of people between 14 to 35 years old that “travels without travelling”, and that uses systematically ICT” (observe for example [www.wiredtourist.com](http://www.wiredtourist.com)). Furthermore, this continuous exploitation of

ICT occurs during touring life cycle (Hawking *et al.*, 2005): planning (location enabled information sharing processes); touring (digital delivery of location based information); reminiscing (after the tour experience and can involve information sharing).

As a result, in each stage it is possible to locate tourists 24 hours a day through equipment and software (Heikkila and Silven, 2004), leading to serious ethical issues relating to personal privacy.

### **ICT for tourism and tourists**

Traditionally, tourism industry has been a leading adopter of innovative technology, which the 2003 Tourism Highlights Report (World Tourism Organization, 2003) have identified four trends: low-cost airlines were rapidly expanding; the Internet dictates information collection and tour booking; the dawn of non-organized touring; the development of “do-it-yourself” travel. From these trends it is possible to acknowledge that information dissemination and exchange are the main inputs for travel industry, which eTourism technologies need to deal (Martini, 2000). Nonetheless, ICT consequences with reference to tourism go far beyond in each phase of touring life cycle:

- planning- communication with prospective clients is often performed through phone, e-mail, chats, or even Skype. Moreover, regional portals allow to access content regarding touring (Jakkilinki *et al.*, 2006), despite the differences that first and second generation tourism portals encompass: dynamic information generation (Kohli and Armstrong, 2006);
- touring- a focus-group survey executed in 2001 by Gartner (Gracia, 2001) in the United States pointed out that over 60 million individuals received location-based advertising messages in exchange for coupons or discounts;
- reminiscing- occurs after the tour experience and can involve sharing of information including recommender systems (Sharda, 2010).

Although, given the overall argument of this paper it is required to debate the potential range of potential Local Based Tourism Systems (LBTS) appliances (Hawking *et al.*, 2005):

- location specific portals- endow expert resources and information to potential tourists about location based service. An example is the Alps website ([www.tiscover.com/](http://www.tiscover.com/));
- tourism tracking- a considerable group of technologies can be referred, namely GPS tracking to support tourists in isolated locations (observe for example [www.geeps.com/](http://www.geeps.com/)); or, integrated software to acknowledge pedestrian-centric content that enables people to orient themselves and navigate efficiently by foot, public transportation systems, or by car, being an example Rich Map Engine ([www.decarta.com/products/mobile\\_rich\\_map\\_engine.htm](http://www.decarta.com/products/mobile_rich_map_engine.htm));
- position based tourism information- the most common application is commentary multilingual systems for exhibitions in museums, national parks, and tours vehicles (an example is [www.equator.ac.ik](http://www.equator.ac.ik)); or, Radio Frequency Identification (RFID) technologies that allows tourists to retrieve information regarding diverse products, receive information concerning hotels and restaurants, etc. (a gigantic and comprehensive application of this technology is the city of Singapore);
- location based recommender systems- provide individualized tourism advice at any stage of the touring lifecycle, being GeoNotes an example.

In conclusion, the newest interaction between tourism and ICT involves the adoption of mobile devices, wireless networks, ubiquitous computing, user-friendly interfaces and location awareness, leading to the promise of personalisation and localisation of tourist activities (Nova, 2004). Nonetheless, despite Berger *et al.* (2004) claim that LBTS are

positive and perhaps extraordinary for inherent mobility in tourism, which Kanellopoulos and Kotsiantis (2007) value chain analysis enhances; the truth, is that pose unforeseen serious ethical issues relating to personal privacy (for further detail see empirical evidences).

## **Control**

### **Etymology**

From the etymological roots of control, it is possible to acknowledge that is a “power” that directly determines a situation; a relation of constraint of one entity (thing or person or group) by another, or, the state that exists when one person or group has power over another (Online Etymological Dictionary, 2001a).

### **The thin bound concerning security**

In a descriptive connotation, security and its components, reproduce the affairs between an object (subject) and its environment, which is consistent with the dual analysis of Introna (1999): externalisation and internalisation of the subject concerning surveillance.

Nevertheless it is imperative to understand that security is normative, an emotionally loaded idea (Mesjasz, 2004). Any endeavour to elaborate an inclusive meaning for security is of course useless, given its extended meanings. In fact, typically security is categorized in: a traditional meaning (security as a characteristic of state); a broader sense (referring directly to a phenomena occurring in international relations, or, security as a public good); and, a universal sense (human security).

Likewise, taking into account an etymological debate a dual outlook arises: the Latin expression is *secures*, meaning safe or secure. Adding the noun *cura* (care), security becomes a quality or state of being secure, or free from danger. This is analogous to Cyncero argument: the absence of anxiety upon which the fulfilled life depends (Liotta, 2002). The subsequent explanation is bounded to the word *securus*, which originally meant liberation from uneasiness, or a peaceful situation without any risks or threats. Nevertheless, the linguistic perception of security is often shaped by cultural elements leading to more interpretations (Morgenthau, 1960). Furthermore, modern surveillance is typically performed through electronic means, leading usually to privacy violation (Brey, 2005). This scenario is a consequence of information retrieval through computer networks, which configure a lack of integrity concerning personal data (Floridi, 2006). Therefore, despite the most widely accepted analysis refers that security and privacy represent more or less a zero-sum logic (Burgess, 2008), the truth is that security regulations imply power relationships and their ethical assumptions (McRobb and Stahl, 2007).

### **Control and personal data fluxes: a political stance**

The issue of personal data protection in modern society is best understood throughout an overview of the laws that regulate personal data security worldwide. The concept of an information society is integrally connected with information and data exchange (Castells, 2000). Despite the various categories of influence and confidentiality, the authors approach personal data of citizens (tourists) that use ICT for each phase of the touring life cycle, as the leading issue of this debate.

In the international sphere it is possible to distinguish a so-called “community”- a group of countries related to each other by more focused ties. Moreover, a regional and functional criterion can be underlined in order to understand these communities: the first group gathers countries that belong to a certain geographical location; the second classifies countries which share common interests (e.g. NATO). As a consequence of this division, universal norms are obligatory for the whole international community, and regional norms are specific for the “community”; although, these overlaps often indulge legislative gaps that could undermine

personal data privacy. In spite of this possibility, the important acts that impact personal data protection are detailed:

Resolution 34/169 UN General Council from 17 December 1979- this document in article IV deals with problems about personal data protection. It contains the collection of directives for officers of the law and government personnel that treat in a daily basis personal data. This data can be only accessible for their official functions, as well as for legal purposes.

Recommendation of the OECD Council from 23 September 1980- this advice of the OECD Council does not have an obligatory character. It is basically a collection of recommendations of the OECD Council regarding solutions that national legislators present as regards to personal data protection in international casus. Nonetheless, the authors paid particular attention to the impact of international exchange of information on global economic development.

Resolution 45/95 UN General Council from 14 December 1990- this is a document containing casus regarding computerized data bases regulation. Once again, the resolutions proposed are not legally binding, because they are simply a collection of proposals regarding guarantees which should be provided in national decrees with regards to computerized storage and propagation of personal data. Among the proposals are setting up conditions for access data by the person involved, as well as security and guarantees against discrimination.

General Declaration of the UNESCO from 11 November 1997- following the fundamentals of this document, there is a need to respect the uniqueness of each person and the differences between people (article 2d). Therefore, any genetic data which allows specific person identification needs to guarantee confidentiality (article 7). It is also declared that genetic data is protected regardless the purpose for their collection (e.g. scientific or, medical research), which conditions are foreseen by law. Additionally, regulates personal data for basic legal acts in European laws.

Directive (EC) nr 45/2001 of the European Parliament and Government from 18 December 2000- this document contains laws regarding individual protection for personal data processing, and free flow between social institutions and organs (article 1). The purpose of this act is to guarantee an effective application of individual's basic rights and freedoms, as well as the easy flow of personal data between Member Countries. Furthermore, the UE has set concrete laws specifically concerning decrees and procedure on data storage and propagation. The overseeing institutions are responsible for meeting out specific sanctions for law infringements, and setting up the European Council for Data Protection.

Directive 2002/58/EC of the European Parliament and Government from 12 July 2002- this directive obliges member countries to guarantee equal levels of protection for basic human rights and freedoms, and in particular the right to personal data privacy in electronic communications. It also obliges them to guarantee the free flow of these data in the community. The regulations of this directive widen and complement the resolutions of Directive 95/46/EC. Aside from this, the regulations of Directive 2002/58/WE guarantee the protection subscribers interests that have legal rights concerning data. This legal act deviates from the earlier Directive 97/66/EC from 15 December 1997 in the matter personal data privacy processing and protection within the telecommunications sector.

Directive 2000/31/EC of the European Parliament and Government from 8 June 2000- this directive regulates the rights and responsibilities of service providers and consumers as

commonly understood in an information-based society. Then, teleinformation services should be transparent and respect consumer's privacy through some special principles for personal data protection. This protection, aside from general principles, imposes that data processing (with certain exceptions) must account consumers consent. For that, data should be limited to the minimum requirements for ensuring contract validity, as well as the user should have the right to remain anonymous or, to use a pseudonym in contracting these services.

Directive 95/46/EC of the European Parliament and Government from 24 October 1995- this is an important document that contains the definition of basic terminologies for personal data, and principles of gathering, collecting, storage and access to data. This document also defines the principles and conditions for legal consent in personal data processing, as well as the legal rights of individuals.

Resolution A/RES/406(XIII) of the World Tourism Organization from 1 October 1999- article 8, number 3 refers explicitly the right that tourists and visitors should benefit the same rights as the native citizens when visiting the country concerning personal data confidentiality, namely when stored electronically.

## **Privacy**

### **The concept**

From the Latin adjective *private* suggests *set apart or, belonging to oneself*; which acknowledges an additional word: *privare* (to separate, individual) (Online Etymology Dictionary, 2001b). Nevertheless, there is little agreement in academic literature about the definition of privacy, because it is certainly a mysterious concept. For example, for Warren and Brandeis (1890: 205) is right "to be let alone", or to Stahl (2004) is the right of informational self-determination.

Some authors like Etzioni (1999) point out two sorts of privacy: informational privacy and decisional privacy. So, an important critic is in order: Etzioni (1999) seems to acknowledge autonomy rather than privacy, which is at some extent explained by Floridi's (2005) ontological interpretation of informational privacy. To Floridi (2005) exist two interpretation theories regarding informational privacy: the reductionist, and the ownership-based. The reductionist declares that informational privacy worth relies on a multiplicity of objectionable consequences that may be caused by its breach; and, ownership-based states that informational privacy needs respect because each person's rights to physical security and property. As a response to this limited analysis, the authors introduce the work of Allen (2003). Anita Allen divides the concept into four dimensional categories: informational (information that forms one's private domain); physical (one's right to self-determination); decisional (it basically means freedom from government or other outside interference with personal life); and proprietary (deals with property interests about the human person).

In conclusion, the elusive perception of privacy derives from the different people's interests: it may be related to control personal information; to physical control; to obtain autonomy; to engage personal development; or even, to safeguard a degree of secrecy (Kemp and Moore, 2007). Despite these arguments one truth is acceptable: privacy is extremely important for a society (Rachels, 1975).

### **Evolution**

ICT development and adoption have been affecting cultural values and promoting an intercultural dialogue between Western and Eastern societies (Collste, 2007). However, it is necessary to shed some light over this intercultural "umbrella" given the existent dissimilar

perspectives regarding privacy: a unique conception as a consequence of intercultural dialogue; and, an opposite perspective.

Authors like Ess (2005; 2006), Hongladarom (2008) or, Nakada and Tamura (2005) have demonstrated that intercultural dialogue has proven to be fruitful, allowing a cultural understanding through the analysis of similarities and differences. As a consequence, a universal concept for privacy will be achievable. On the other hand, Brey (2007) declares the concept of privacy is inexistent in Eastern cultures, due to their social construction as a collective culture, which at some extent the work of Orito and Murata (2007) supports. Therefore, an important question arises: which perception could help the authors to understand tourist's personal privacy? This is important because travellers exist worldwide, and it is reasonable to understand if their perception of privacy can promote different issues as regards to locational privacy. To the authors the answer is quite simple: only the mishmash of both conceptions translates positive and complementary results. In spite of this scenario be achievable, is again the authors' opinion that these perceptions are acknowledging different analytical dimensions (Stahl's matrix conversion) (Stahl, 2002):

- the unique conception- is on a "normative/theoretical" level. This claim is supported at some extent by the work of Himma (2008). In his work, *The intercultural ethics agenda from the point of view of a moral objectivist*, Kenneth Himma points out that moral objectivism provides a superior foundation for the normative debate for intercultural information ethics;
- the opposite perspective- is on a "descriptive/practical" level. This is suggested for example through the work of Mizutani *et al.* (2004).

Therefore, for a positive and comparable theoretical diversity it is required that firstly both perspectives entail the normative level and afterwards to understand practical implications of this diversity, in order to permit an inclusive answer.

## **Dimensions**

In accordance to the International Telecommunication Union (2005), informational privacy acknowledges three domains that simultaneously are distinct, but necessarily related: technical (underlines design issues related to such areas as network security and user interface design); regulatory (outlines privacy as regards to data protection and related statutes and regulations); and, sociological (considers privacy as a social issue related to cultural practices, ethics, and institutions). However, regardless the policy analysis exist a continuous tension between personal privacy and societal control. This is a result of privacy be a crucial human basic right (Rogerson, 1998), which can be under an intrinsic or instrumental scope. Thus, privacy not just permits us to develop healthy interpersonal relationships, but also a requirement for democratic state (Stahl, 2007).

## **Empirical evidences**

### **Overview**

Despite the previous sections it is necessary to address an important issue: how can we define locational privacy? And, which are its features? For Saha and Mukherjee (2003), is considered as an essential component for the development and delivery of context-aware services to mobile and nomadic users. To Danezis *et al.* (2005), is a set of data that describes an individual's location over a period of time. The time and location resolution vary with the technology used to collect the data. Even so, the authors will follow Blumberg and Chase (2007) definition: ability of an individual to move in public space with the reasonable expectation that their location will not be systematically and secretly recorded for later use. Hence, locational privacy engages two critical dimensions: locational awareness, and

technology. According to Duckham and Kulik (2006) locational awareness concerns the utilization of information with reference to an individual's current location to grant additional relevant information and services to that individual, being a specific type of context-awareness. In fact, the concept context overloads an individual's physical, social, physiological, or emotional circumstances (Schmidt *et al.*, 1999). On the other hand, given the research aim of this contribution technology encompasses LBTS applications, as for instance for: navigation (directions, traffic control); information exchange (travel and tourist guides); tracking (people, vehicle or product tracking); advertising (advertisement alerts); and, social networking (locating friends, instant messaging).

### **Crime scene investigation: a metaphorical analysis!**

To become a serious detective is fundamental to observe and analyse carefully a crime scene in order to obtain keen evidences (following subsection). From the overall argument, is feasible to proclaim that location-based experiences extend digital media out into the physical world (Benford, 2005); and, the multiple contexts and LBTS appliances configure a Janus perspective (Floridi, 2006), because in spite of allow real time access to information and content, allow collect field data, and promote experiences personalisation; the truth is that, seriously endanger tourists locational privacy due to a constant flux of personal data throughout multiple platforms. This crime scene is perfectly illustrated in literature:

- LTBS potential- Girardin *et al.* (2008) combined data from Flickr to understand the areas of tourist's concentration, their temporal signatures and activities; and, Hinze and Voisard (2003) demonstrate the potential of Event Notification Systems;
- locational privacy issues- applying privacy on the dissemination of locational information (Marias *et al.*, 2006); and, privacy concerns in location based services (Gadzheva, 2007).

Even so, the authors introduce some keen empirical exhibits to allow a reliable investigation.

### **Keen exhibits**

Exhibit A- Olympic Navigator was a locational based service to support tourists during the Olympic Games of 2004, which positively possessed a policy concerning personal data. The system created a pseudonym, which was given a public key through cryptography to enable a strong authentication, confidentiality and integrity. Likewise, the policy entailed an authorization to maintain tourist's data during five days. The problem relied on a basic algorithm, Trivial Secret Sharing, that secretly allowed tracking the different tourist pseudonyms, and it was not stated into the personal data policy. Therefore, it was possible to track tourist's location!

Exhibit B- during a recent stay in United Kingdom, one of the co-authors has received a text message by its global mobile operator alerting that his choice concerning the local operator was not under the umbrella of its international calls. From this information the Reader may consider odd or inappropriate this example; however, it becomes relevant after novel information: the text message also referred which were the local operators in the co-author geographical position! Finally, the co-author stresses out that his personal experience happened on January 25, 2010.

Exhibit C- another critical example happened during the same stay: on January 26, 2010 the co-author received a call by the global operator support concerning a pending administrative issue. Again, at a first glimpse it seems a non-problematic issue; yet, it was the co-author intention to notify the global operator not to charge this call because it was abroad. Although,

amazingly before this announcement the global operator have informed the co-author that this call would not be charged given its current geographical location!

Exhibit D- through continuous informal meetings with a major producer of electronic and communications systems, one of the co-authors have concluded that plentiful hotels misuse personal data that is collected, when travellers use their networks. Moreover, after analysing several hotels websites it was denoted that most do not have privacy/confidentiality policies.

Exhibit E- LandLoc is a software for mobile devices that permits to a user choose landmarks for an object: building, shop, a park, etc. Afterwards, the software creates a three dimensional electronic representation of the physical space, and presents the best solution through the triangulation of user's location, chosen landmarks and topography of the region. The following step is to act like a GPS using mobile network, meaning that is possible to track permanently the tourist during its trajectory.

## **Discussion**

### **Act 1: preparing the “case”**

As mentioned above, locational privacy and data protection denotes social and ethical grounds. Privacy issues entail location profiling, tourist tracking, and information relevance; LTBS social implications occur through mainly during touring and reminiscing phases. So, the right to secure locational privacy is critical and to achieve it literature acknowledges several formal models and technologies. Examples of formal models are: visibility classification scheme (Jarvinen *et al.*, 2002), and anonymization model (Shin *et al.*, 2008); and, for technologies are: semantics-aware obfuscation (Damiani *et al.*, 2008), and location sensor networks (Gruteser *et al.*, 2003). Moreover, personal data fluxes through digital networks (including LTBS) are monitored and secured through the Echelon system (Bierzanek and Symonides, 2005), which can be bounded to the claim of Etzioni (1999) that an individual's right to privacy is somehow conferred by the society; and, therefore leading to a necessary future debate about individuals and institutions moral obligations.

### **Act 2: the “court's” decision**

Following Hawking *et al.* (2005), LTBS market stakeholders assume three basic categories: infrastructure providers (hardware, software and network infrastructure providers); tourism providers (include travel agents, airlines, itinerary providers, hospitality providers, vehicle rental providers and various government agencies); tourism content providers (act as content enablers connecting providers and tourists); and, consumers (tourists that seek out for information). In spite of this scenario all stakeholders have moral obligations, which imply responsibility and its conditions as an answer to ethical problems (Stahl, 2004). To acknowledge these moral obligations Duckham and Kulik (2006) work pertaining to strategies for protect locational privacy are the key to unlock the “court's” decision:

- regulatory strategies- encompasses the development of rules to govern fair use of personal information;
- privacy policies- are trust-based methods for forbid certain uses of location information. Whereas regulation aims to provide global or group-based guarantees of privacy, privacy policies aim to provide individual privacy;
- anonymity- concerns the dissociation of information about an individual and its actual identity. The most common form of protection is to associate an pseudonym;
- obfuscation- demeaning locational information quality, with the aim to protect it. However, Duckham (2008) demonstrates that after 100 simulations its reliability diminishes 30 per cent.



On the other hand tourists are willing to share information, although with who and until what extent are the fundamental queries? According to Olson *et al.* (2005) it is possible to cluster peoples' sharing willingness into categories; nevertheless, is extremely difficult to determine what is an achievable and desirable level of access by others regarding wired tourists locational information (future research scenario). Likewise, it is the authors' opinion that locational privacy does not symbolize the complexity and interaction between global and local systems (stakeholders, technologies and regulations). Therefore, glocal privacy emerges as a new buzzword.

## Conclusion

From the overall arguments of this contribution it seems reasonable to claim that the authors have proven that locational privacy resumes the trade-off between traveller's mobility, societal control for security reasons, and tourist's informational requests; besides, it resumes a statement or an argument based on a false/invalid inference (fallacy). In spite of these claims it is crucial to shed some light over the following thoughts: it is required an empirical shift concerning privacy normative horizons; personal locational information (PLI) concept needs a further and incessant debate; LTBS design seems to neglect or claim for eureka in control mechanisms regarding PLI, and for that generate unique privacy issues; it is remarkably complex for individuals (tourists) be in control of his location data, as well as to understand until what extent service providers exploit this information; national and international agencies must engage a serious debate concerning locational privacy specificity, in order to evolve the existent laws.

Concluding, in *Mandragola* Machiavelli's comic play, it is possible to feel the spirit of modern science without any of its apparatus. Additionally, in his *Discourses on Livy* lead us to wrap up that to secure and perpetuate the republic (society) is essential to adhere to a new formula: lower moral standards improve society chances of be secure and achieve better results. In fact, locational privacy issues seem to replicate this idea which is exceptionally dangerous for individuals. Therefore it is required an urgent debate and countermeasures, otherwise the panoptic effect of Bentham will become a reality.

## Acknowledgements

The first co-author of this paper would like to thanks ISLA Leiria for its financial assistance with reference to ETHICOMP 2010.

## References

- Allen, A. (2003), Privacy, in LaFollette, H. (ed), *The Practical Handbook of Practical Ethics*, Oxford, NY: Oxford University Press, 485-513.
- Benford, S. (2005), *Future location-based experiences*, JISC Technology and Standards Watch, London.
- Berger, H., Dittenbach, M. and Merkl, D. (2004), User-oriented evaluation of a natural language tourism information system, *Information Technology & Tourism*, 6, 3, 167-180.
- Bierzanek, R. and Symonides, J. (2005), *Public international law*, LexisNexis Publisher, Warsaw.
- Blumberg, A. and Chase, (2007), *Electronic tolling and locational privacy: How to make e-pass preserve locational privacy*, Stanford University, online at <http://math.stanford.edu/~blumberg/traffic/secureEZ.pdf>, accessed 10.01.2010.
- Brey, P. (2005), Editorial introduction- Surveillance and privacy, *Ethics and Information Technology*, 7, 4, 183-184.

- Brey, P. (2007), Is information ethics culture-relative, *International Journal of Technology and Human Interaction*, 3, 3, 12-24.
- Burgess, P. (2008), *Security after privacy: The transformation of personal data in the age of terror*, International Peace Research Institute, Oslo.
- Carlvik, O. and Jonsson, I.-M. (2001), Virtual tourist based on PeerRing- communicating with people you have never met, in Stephanidis, C. (ed), *Universal Access in Human Computer Interaction- Towards an Information Society for All (Vol. 3)*, Norwood, NJ: Ablex Publishing Corp, 271-275.
- Castells, M. (2000), *The rise of the network society: The information age: economy, society and culture (vol 1)*, 2<sup>nd</sup> ed, Blackwell, Malden, MA.
- Collste, G. (2007), Globalisation, ICT-ethics and value conflicts, in Bynum, T. *et al.* (eds), *ETHICOMP 2007 (vol 1)*, Tokyo: Meiji University, 91-99.
- Damiani, M., Bertino, E. and Silvestri, C. (2008), Protecting location privacy through semantics-aware obfuscation techniques, in Karabulut, Y. *et al.* (eds), *Trust Management II*, Boston, MA: Springer, 231-245.
- Danezis, G., Lewis, S. and Anderson, R. (2005), How much is location privacy worth?, Paper presented at the 4<sup>th</sup> Workshop on the Economics of Information Security, Cambridge, MA: USA.
- Duckham, M. (2008), Location privacy protection through spatial information hiding, Office of the Victorian Privacy Commissioner, online at [http://www.privacy.vic.gov.au/privacy/web.nsf/download/FD2EADCF697270F8CA2574A4001CD15A/\\$FILE/Matt%20Duckham%20PVN%20meeting%20160708.pdf](http://www.privacy.vic.gov.au/privacy/web.nsf/download/FD2EADCF697270F8CA2574A4001CD15A/$FILE/Matt%20Duckham%20PVN%20meeting%20160708.pdf), accessed 15.01.2010.
- Duckham, M. and Kulik, L. (2006), Location privacy and location-aware computing, in Drummond, J. *et al.* (eds), *Dynamic & Mobile GIS: Investigating Change in Space and Time*, Boca Rator, FL: CRC Press, 34-51.
- Eagle, N. and Pentland, A. (2006), Reality mining: Sensing complex social systems, *Personal Ubiquitous Computing*, 10, 4, 255-268.
- Ess, C. (2005), Lost in translation?: Intercultural dialogues on privacy and information ethics (Introduction to special issue on Privacy and Data Privacy Protection in Asia), *Ethics and Information Technology*, 7, 1, 1-6.
- Ess, C. (2006), Ethical pluralism and global information ethics, *Ethics and Information Technology*, 8, 4, 215-226.
- Etzioni, A. (1999), *The limits of privacy*, Basic Books, New York, NY.
- Floridi, L. (2005), The ontological interpretation of information privacy, *Ethics and Information Technology*, 7, 185-200.
- Floridi, L. (2006), Information technologies and the tragedy of good will, *Ethics and Information Technology*, 8, 4, 253-262.
- Gadzheva, M. (2007), Privacy concerns pertaining to location-based services, *International Journal of Intercultural Information Management*, 1, 1, 49-57.
- Girardin, F. *et al.* (2008), Understanding of tourist dynamics from explicitly disclosed location information, *Journal of Location Based Services*, 2, 1, 41-56.
- Gracia, D. (2001), *The strings attached to wireless advertising: a tutorial (market)*, Gartner Group, Stanford, CT.
- Gruteser, M. *et al.* (2003), Privacy-aware location sensor networks, in Sankoff, D. and Kruskal, J. (eds), *Proceedings of the 9<sup>th</sup> Conference on Hot Topics in Operating Systems*, Berkeley, CA: USENIX Association, 28-28.
- Hawking, P. *et al.* (2005), Emerging issues in location based tourism systems, in Unhelkar, B. (ed), *Proceedings of the International Conference on Mobile Business*, Washington, DC: IEEE Computer Society, 75-81.

- Heikkilä, J. and Silven, O. (2004), A real-time system for monitoring of cyclists and pedestrians, *Image and Vision Computing*, 22, 7, 563-570.
- Himma, K. (2008), The intercultural ethics agenda from the point of view of a moral objectivist, *Journal of Information, Communication & Ethics in Society*, 6, 2, 101-115.
- Hinze, A. and Voisard, A. (2003), Location- and time-based information delivery in tourism, in *Lecture Notes in Computer Science, Advances in Spatial and Temporal Databases* (vol 2750), Berlin: Springer, 489-507.
- Hongladarom, S. (2008), Floridi and Spinoza on global information ethics, *Ethics and Information Technology*, 10, 2/3, 175-187.
- International Communication Union (2005), Privacy and ubiquitous network societies, International Communication Union, online at <http://www.itu.int/osg/spu/ni/ubiquitous/Papers/Privacy%20background%20paper.pdf>, accessed 12.01.2010.
- Introna, L. (1999), Privacy, autonomy and workplace surveillance, *The ETHICOMP Journal*, online at [http://www.ccsr.cse.dmu.ac.uk/journal/articles/vol3iss2\\_20](http://www.ccsr.cse.dmu.ac.uk/journal/articles/vol3iss2_20), accessed 30.12.2009.
- Jakkilinki, R., Sharda, N. and Ahmad, I. (2006), Ontology based intelligent tourism information systems: An overview of development methodology and applications, in Cooper, C., De Lacy, T. and Jago, L. (eds), *Leading-edge Developments in Tourism ICT and Related Underlying Technologies*, Queensland: Sustainable Tourism CRC, 2-9.
- Jarvinen, O., Earp, J. and Antón, A. (2002), A visibility classification scheme for privacy management requirements, Paper presented at the 2<sup>nd</sup> Symposium on Requirements Engineering for Information Security, Raleigh: NC, USA.
- Kanellopoulos, D. and Kotsiantis, S. (2007), Wireless multimedia communications impacts on tourism destination value chain, *Journal of Engineering and Applied Sciences*, 2, 1, 161-169.
- Kansa, E. and Wilde, E. (2008), Tourism, peer production, and location-based service design, in Wang, C. (ed), *Proceedings of the 2008 IEEE International Conference on Services Computing* (vol 2), Washington, DC: IEEE Computer Society, 629-636.
- Kemp, R and Moore, A. (2007), Privacy, *Library Hi Tech*, 25, 1, 58-78.
- Kohli, G. and Armstrong, L. (2006), Location based services and mobile applications, in Cooper, C., De Lacy, T. and Jago, L. (eds), *Leading-edge Developments in Tourism ICT and Related Underlying Technologies*, Queensland: Sustainable Tourism CRC, 11-21.
- Liotta, P. (2002), Boomerang effect: The convergence of national and human security, *Security Dialogue*, 33, 4, 473-488.
- Marias, G. et al. (2006), Applying privacy on the dissemination of location information, *Telematics and Informatics*, 23, 3, 211-225.
- Martini, U. (2000), ICTs as competitive drivers for new destination management concept, in Kreilkamp, E. *et al.* (eds), *Gemachter oder Gelebter Tourismus? Destinations Management and Tourismus Politik*, Linde: Vienna, 141-166.
- McRobb, S. and Stahl, B. (2007), Privacy as a shared feature of the e-phenomenon: a comparison of privacy policies in e-government, e-commerce and e-teaching, *International Journal of Information Technology and Management*, 6, 2/3/4, 232-249.
- Mesjasz, C. (2004), Security as a property of social systems, *AllAcademic*, online at [http://www.allacademic.com/meta/p72561\\_index.html](http://www.allacademic.com/meta/p72561_index.html), accessed 15.01.2010.
- Mizutani, M., Dorsey, J. and Moor, J. (2004), The internet and Japanese conception of privacy, *Ethics and Information Technology*, 6, 2, 121-128.
- Morgenthau, H. (1960), *Politics among nations. The struggle for power and peace*, Alfred A. Knopf, New York, NY.
- Nakada, M. and Tamura, T. (2005), Japanese conceptions of privacy: An intercultural perspective, *Ethics and Information Technology*, 7, 1, 27-36.

- Nelson, B. (2009), Computer has eye for suspicious behaviour- Tourist or terrorist?, MSNBC, online at <http://www.msnbc.msn.com/id/28566179/>, accessed 10.01.2010.
- Nova, N. (2004), Locative media: A literature review, Craft Research Report 2, École Polytechnique Fédérale De Lausanne, Lausanne.
- Olson, J., Grudin, J. and Horvitz, E. (2005), Toward understanding preferences for sharing and privacy, in Veer, G. and Gale, C. (eds), Conference on Human Factors in Computing Systems, Portland, OR: ACM, 1985-1988.
- Online Etymology Dictionary (2001a), Control, Online Etymology Dictionary, online at <http://www.etymonline.com/index.php?search=control&searchmode=none>, accessed at 14.12.2009.
- Online Etymology Dictionary (2001b), Privacy, Online Etymology Dictionary, online at <http://www.etymonline.com/index.php?l=p&p=33>, accessed 15.12.2009.
- Orito, Y. and Murata, K. (2007), Rethinking the concept of information privacy: A Japanese perspective, in Bynum, T. *et al.* (eds), ETHICOMP 2007 (vol 2), Tokyo: Meiji University, 448-455.
- Oxford Dictionary (2008), Oxford English dictionary, Oxford University Press, Oxford.
- Rachels, J. (1975), Why privacy is important, *Philosophy and Public Affairs*, 4, 4, 323-333.
- Rogerson, S. (1998), Ethical aspects of information technology- Issues for senior executives, Institute of Business, London.
- Saha, D. and Mukherjee, A. (2003), Pervasive computing: a paradigm for the 21<sup>st</sup> century, *IEEE Computer Magazine*, 36, 3, 25-31.
- Schmidt, A., Beigl, M. and Gellersen, H-W. (1999), There is more to context than location, *Computers & Security*, 23, 6, 893-901.
- Sharda, N. (2010), Tourism informatics- Visual travel recommender systems, social communities, and user interface design, IGI Global, Hershey, PA.
- Shin, H., Atluri, V. and Vaidya, J. (2008), Profile anonymization model for privacy in a personalized location based service environment, in Carriço, L., Baloian, N. and Fonseca, B. (eds), Proceedings of the 9<sup>th</sup> International Conference on Mobile Data Management, Washington, DC: IEEE Computer Society, 73-80.
- Staab, S. and Werthner, H. (2002), Intelligent systems for tourism, *IEEE Intelligent Systems*, 17, 6, 53-64.
- Stahl, B. (2002), Ethical issues in e-teaching: A theoretical framework, De Montfort University, online at [www.cse.dmu.ac.uk/~bstahl/publications/2002\\_Ethics\\_eteaching\\_framework.PDF](http://www.cse.dmu.ac.uk/~bstahl/publications/2002_Ethics_eteaching_framework.PDF), accessed 10.01.2010.
- Stahl, B. (2004), Responsibility for information assurance and privacy, *Journal of Organizational & End User Computing*, 16 3, 59-77.
- Stahl, B. (2007), Privacy and security as an ideology, *IEEE Technology and Society Magazine*, 26, 1, 35-45.
- Warren, S. and Brandeis, L. (1890), The right to privacy, *Harvard Law Review*, 5, 193-220.
- Wolf, J. (2004), Applications of new technologies in travel surveys, Paper presented at the 7<sup>th</sup> International Conference on Travel Survey Methods, Playa Herradura: Costa Rica.
- World Tourism Organization (2003), Tourism highlights- Edition 2003, World Trade Organization, Madrid.
- World Tourism Organization (2009), World tourism barometer (vol 7), World Trade Organization, Madrid.
- World Travel and Tourism Council (2007), Terms and conditions of use and legal disclaimer, World Travel and Tourism Council, online at [http://www.wttc.org/eng/Contact\\_WTTC/Privacy\\_Statement/](http://www.wttc.org/eng/Contact_WTTC/Privacy_Statement/), accessed 15.01.2010.