Ethical and Political Responsibility in Location Based Services - The Need of Implementing Ethical Thinking in Our Research Field

Franz Obex*, Guenther Retscher**

* Freelancer, Vienna, Austria; obex@chello.at
** Department of Geodesy and Geoinformation, Vienna University of Technology, Austria; guenther.retscher@tuwien.ac.at

Abstract. Rapid technical developments in Location Based Services (LBS) lead to new applications and possibilities in many personal and institutional sectors. LBS became a powerful instrument in predicting consumer behaviour and preventing crime. The dichotomy between privacy and security leads to new ethical issues that have to be addressed. We are willing to reveal our personal data at many occasions to get a small benefit or more convenience in daily life. Although we are always lagging behind the latest developments in respect to data protection and the privacy issue, the politics constantly has to adopt the law with regards to LBS, privacy and anonymity. The trend is towards continuous localisation and tracking of certain people or even the whole population. Users of electronic devices should get the right to withdraw their consent for transferring location based and other personal data at any time. They also should get clear and comprehensive information when and for what they give away their personal data and location and their further use. The LBS research community should keep privacy and ethical implications in mind from the very beginning of their research projects and already ongoing research activities. Meanwhile LBS influences every individual's life, hence ethical issues have to be debated within the research community and taught our students. Technical Universities and especially the developers of LBS can no longer keep their credibility without cooperating with ethical experts or an ethical committee.

Keywords. Privacy, Values and Norms, Ethical Committee, Politics

Published in "Proceedings of the 11th International Symposium on Location-Based Services", edited by Georg Gartner and Haosheng Huang, LBS 2014, 26–28 November 2014, Vienna, Austria.

1. Introduction

When we talk about LBS most technical researchers imply that it is mainly about further enhancing technologies and algorithms including the development of new advanced Apps to improve personal navigation and to deliver location oriented information just in time to a single person or group of users. Technical developments of GNSS and other ubiquitous positioning methods can become a very powerful tool when tracking an individual or a whole population based on automated algorithms. Ng-Kruelle et. al. (2002) elaborate it to the point in their paper "The Price of Convenience: Privacy and Mobile Commerce" that due to technical developments users are often only vaguely aware of the fact that they transmit their current location and trajectory to navigation and guidance service providers while at the same time receiving aggregate information based on data transmitted by other users. In the following we pick up current developments with regards to ultimate users and the LBS community where we question if the researcher and provider have taken privacy and data protection into account adequately.

For instance, in emerging Intelligent Transport Systems (C-ITS), the positions of all road users have to be transferred to and used by the service provider in order to improve road safety and efficiency of the road network. New technologies, such as cooperative positioning (CP) (or also referred to as collaborative positioning) of a group of users (see e.g. Grejner-Brzezinska and Toth, 2013) are developed in particular, to deliver more robust positioning performance and to increase positioning quality using shared information between the users that operate within a defined neighbourhood (Kealy et al., 2014). Such developments show that user's privacy frequently is exchanged for convenience. Ng-Kruelle et. al. (2002) state that individual consumers of such navigation services must always balance costs (e.g. loss of privacy pertaining to personal location and driving speed) against benefits obtained (e.g. navigational support, improved road safety, collision avoidance, etc.).

Apart from commonly employed standard LBS services and the provision of navigation support, several worldwide researchers are focusing on the analysis of the movement behaviour of pedestrian users using cellular phone data. Typical examples of investigated application fields include the determination of commuting patterns for downscaling of movements in road or street canyons, tracking of large crowds at mass events, studies of tourist behaviours, shoppers, public transport users, etc. Here it is often stated that the anonymity of the users is or shall be guaranteed. Researchers in Estonia (see e.g. Saluveer and Ahas, 2010) are using passive cellular phone data from a major provider for their studies. In contrast to active

mobile positioning where the location of the cellular phone is asked following a specific query, passive positioning data is automatically stored in memory or log files of mobile operators (i.e. billing memory, hand-over between network cells, home location register, etc.) to the precision of network cells. The database of passive positioning data used in the studies is the locations of all 'calls out' (calls initiated by the respondent, not received calls) (see Ahas et al., 2010). The assigned random ID, generated by the operator, which is not related to phone or SIM card number, but remains constant for every phone, enabled them to identify the calls made by one person.

Hence, this possibility enables the researchers to link the person's calls throughout the whole study period. In this case the ultimate consumer has no choice to give his informed consent to put his data at disposal or to disagree, since he doesn't even know that his data is being used to analyze several aspects and to be turned into a source for population statistics. Such a course of action poses a severe threat for cellular phone holders as the random ID assigned to them keeps constant over a whole study period. Mobile operators can then aggregate personal and private geographical data from log files, such as location points or movement vectors. Mascetti et al. (2007) argue that "in general, the association between the real identity of the user issuing an LBS request and the request itself, as it reaches the service provider, can be considered a privacy threat. [...] Simply dropping the issuer's personal identification data may not be sufficient to protect user's privacy". Therefore it should become mandatory to inform LBS users when and what for they are giving away their personal data and location information but that they also have the right of refusal.

The remainder of the paper is organized as follows: The price of convenience which LBS users pay is elaborated in section 2 followed by a brief discussion of adopted anonymisation strategies for privacy protection in LBS in section 3. The struggle between maintaining privacy versus security is discussed in section 4. Then in section 5 legislative and political activities in the context of maintaining and protecting user's privacy aspects are reviewed. In the concluding remarks (section 6) the need and postulate for the establishment of ethical committees at Technical Universities and/or the cooperation with social scientists is raised.

2. The Price of Convenience

The publicist Frank Schirrmacher (Quarks & Co, 2014) argues that we are almost unperceived navigated on the internet. For instance, advertisements that are placed on the result page of a search engine, a book recommenda-

tion on an online booksellers start page that might be interesting, or a personalised add sent home by a discounter in dependence of changing shopping habits of users due to changes in their life. An example would be a reaction to pregnancy of a user. This happened to 16 year old girl in the US whose parents found out that she is pregnant because of all kind of baby advertisements suddenly were addressed to their daughter (Quarks & Co, 2014). Every day more and more data is collected from us, turning us into specific usable 'profiles'. Meanwhile every one of us is registered in several profiles, whether it is shopping habits at the discounter, buying tickets for cultural events on the internet, search terms in search engines, cookies from web pages, surveillance cameras in public, and so on.

The population is beginning to get aware of that. More or less conscious and with an astounding indifference, many people are willing to give away and to disclose their data for a small benefit or convenience. They negate the fact that all their data is collected. There is a possibility that we may be intercepted, monitored and tracked. 74% of the Europeans see disclosing personal information as an increasing part of modern life (European Commission, 2011).

"Digital technologies are setting down the new grooves of how people live, how we do business, how we do everything" (Lanier, 2013). Quite a lot of LBS are and certainly will be based on that life style. "We want free online experiences so badly that we are happy to not be paid for information that comes from us now or ever". Lanier (2013) and many researchers for LBS strive for a future where..."In a world of digital dignity, each individual will be the commercial owner of any data that can be measured from that person's state of behavior".

One application of LBS ended up in that parents track their children enforcing them to answer their phone call, otherwise they can remotely deactivate their mobile device. These children are socialized in being tracked down all the time and we do not know how this will change the next generation's habits and understanding on privacy. Justice Louis Brandeis, cited in Lanier's Book "Who Owns the Future", (2013) gives us a rather radical definition of privacy. It is the "right to be left alone". It is up to us to set limits and to initiate a broad discussion on the use of our data with regards to our privacy and its ethical and political dimensions. Values shape people's decisions, which in turn, determine human destiny. Any influence on human values is a potential influence on the future (Sperry, 1983).

What we define as privacy and intimacy today is far from 100 years ago. Our research outcomes are shifting and shaping common standards, constantly influencing political and social structures as well as decisions, no matter if we come from the 'hard' or 'soft' sciences.

3. Anonymisation Approaches for Privacy Protection of LBS Users

Several researchers raise major concerns for the protection of personal location information of LBS users. Damiani et al. (2009), for instance, described an approach where the user's privacy is protected based on forwarding the LSB provider a coarse instead of the actual user location. This strategy is termed as 'obfuscation'. Commonly employed techniques for privacy preservation are spatial cloaking methods or spatial generalisation and they are briefly introduced and discussed in the following.

Spatial cloaking is extensively applied to provide spatial k-anonymity. In general, k-anonymised means that each record is indistinguishable from at least k-1 other records with respect to certain identifying attributes. As defined by Kalnis et al. (2007) this concept means in the context of LBS: "given a query, guarantee that an attack based on the query location cannot identify the query source with probability larger than $1/k$, among other k-1 users". In order to prevent privacy violation, the LBS user can avoid providing his exact location and, instead, send to the service provider not his personal data but a generalised area that includes his location and the location of other k-1 users. The LBS provider then replies to this generalised request with the queried result which is the closest one to any point of the generalised area. Hence, the ID and exact position of an individual is replaced by an anonymising spatial region (ASR) (also termed as cloaked region CR) containing the client that issued the query and k-1 other users, while the privacy metric is defined by the probability $1/k$ of identifying a user in the respective ASR. In other words, then a set of candidate results that satisfy the query condition for any possible point in the ASR is sent by the anonymiser to the LBS user.

Damiani et al. (2009) used the example that a person's health problems may be revealed if the person is currently inside or very close nearby to a hospital. A hospital defined as ASR is obviously a sensitive place for certain users. The authors demonstrate and argue that "privacy breaches may occur because existing obfuscation techniques are unable to protect against the inferences made by linking the geometric information with the semantic location which, depending on the perceptions of users, may represent sensitive information. Thus protection of sensitive location information requires techniques that are able to take into account the geographical context in which users are located, in particular the semantic locations and the spatial distribution of population, as well as the users' privacy preferences". Hence, using such comprehensive techniques for the protection of location privacy against location inference attacks the LBS subscribers can specify location

privacy preferences about the places that they consider sensitive as well as the desired degree of privacy protection.

Spatial generalisation is comprehensively discussed and assessed in Mascetti et al. (2007). The typical scenario assumes the existence of a so-called Location-aware Trusted Server (LTS). The server stores precise location data of all *k* users, using data directly provided by them. Hence, the LTS has the ability to efficiently perform spatio-temporal queries to determine which or how many users are in a certain region. Then the LBS provider fulfils user requests and communicates with the user through the LTS. The answer from the service provider is routed through the LTS to be redirected to the specific user with a refined result (Kalnis et al., 2007; cited in Mascetti et al., 2007). The three main goals in such an anonymisation approach are: (a) to guarantee the user's privacy by ensuring that a sufficiently large number of potential users are not distinguishable from the issuer; (b) to preserve the quality of service by minimising the size of the ASR area; and (c) to be efficient, since it must be computed online (Mascetti et al., 2007). As the first two goals are somehow contrary to each other regarding the size of the ASR and therefore are partly difficult to be achieved at the same time because of limited processing time and power, a LBS query result may not be very precise and satisfy the user when he receives too many search results which are not relevant to his current location. Considered that only a few other users are present at one time and they are spatially far apart from each other, the ASR will be quite large. In this case, the user will only receive imprecise results from the service.

Kalnis et al. (2007) identified other challenging problems associated with such generalisation algorithms. In cases where a user issues continuous similar LBS queries it is difficult to preserve anonymity when the same query from successive locations is asked. Then it is likely that an attacker can disclose the identity of the querying user. Further problems may arise when the attacker has additional information about the preferences of a certain user. The following example is used by Kalnis et al. (2007): when a rugby fan is asking for the location of the nearest rugby club and his ASR contains only other female users in addition to him, the attacker may infer him as query source with higher probability.

As can be seen from the examples described above anonymisation approaches have several shortcomings and are not able to completely guarantee the anonymity of a LBS user. "In practice, users would not be reluctant to access a service that may disclose their political/religious affiliations or alternative lifestyles" said Kalnis et al. (2007). Especially users currently located at sensitive places, such as in a hospital (see example from Damiani et al., 2009), normally are not willing to reveal their precise location and

give up their privacy completely. Hence, further research and developments are required for privacy protection of LBS users followed by an investigation about the users' willingness to give away their data. In the following section the ambivalence between maintaining privacy of a person versus security is discussed.

4. The Strive for Maintaining Privacy versus Security

Beresford and Stajano (cited in Kido et al., 2005) point out that location privacy is "the ability to prevent other parties from learning one's current or past location" thus the "protection of location privacy is one of the most significant issues of LBS". Location technologies developed over the years, such as GNSS, cellular location-based solutions, indoor positioning systems, etc., have resulted in new services that make use of both location-based and context-awareness. Enabled by modern telecommunication technology, convenient services promote changes of lifestyle, thus 'total' privacy is increasingly difficult – perhaps impossible – to maintain. The benefit offered by each 'convenience' is in general associated with a loss of privacy – that is, services can only be effectively provided when the service provider has access to the consumer's location, personalisation data, or both (see Ng-Kruelle et al., 2002).

Meanwhile LBS are much more than every one of us can imagine. It is possible to retroactively track an individual by creating its movement behaviour and profile. It is a highly fractured scientific field where one research group, e.g. technical or social scientists, geodesists, geographers, cartographers, App developers, etc., sometimes only vaguely knows the results of other research teams, not taking into account that their results in conjunction with the results of another team can be used to create a totally new and questionable tool. Nowadays LBS data became part of a lucrative business for trusts like Google, Apple, Samsung, etc. They are of striking military interest and of equal interest for intelligence services. LBS data can be turned into a powerful instrument, when e.g. at the first sight harmless data and tools that have been developed in LBS research projects are brought together and merged. Politicians and police departments are using LBS generated data for controlling parts of cities and suspicious citizens. The collection of big data and data mining are wide spread and most of us do not know when and which data of us is collected. That also happens with data we generate and track for LBS. It seems likely that within the next following five to ten years, when looking at the sky, we might see five Unmanned Aerial Vehicles (UAV's), three of them are delivering parcels but the other two are following us at every move we make turning us into

suspects. This scenario is an example for how important it is to critically consider and to question the technology that we develop with regards to political and social effects, not to mention their liability for abuse. This implies the need to discuss potentially negative effects within our own research community and with social scientists to publish our warnings. We argue that it needs a further step towards an ethics committee to investigate together with social scientists the social, political and ethical dimensions of a new research project and its possible outcomes.

What can be seen from Figure 1 is one and the same part of a city with four different data sets such as social structure, crime rate, unemployment rate and former detainees that can be merged for a certain district. In the U.S., such programs are already in use in some cities. In Chicago, the forecast is derived from analyses of social networks and the criminal files of recent years. The police computer creates a so called 'heat list' with the 400 most dangerous citizens of the city. The list specifies who may be involved most likely at the next shooting or major crime. The police visits these citizens for prevention purposes and warns them not to commit serious crimes. So on one hand the population in such high crime hotspots loses a part of their privacy, on the other hand the police can grant more security. In fact due to this measures in Chicago the crime rate dropped by 38% (Quarks & Co, 2014).

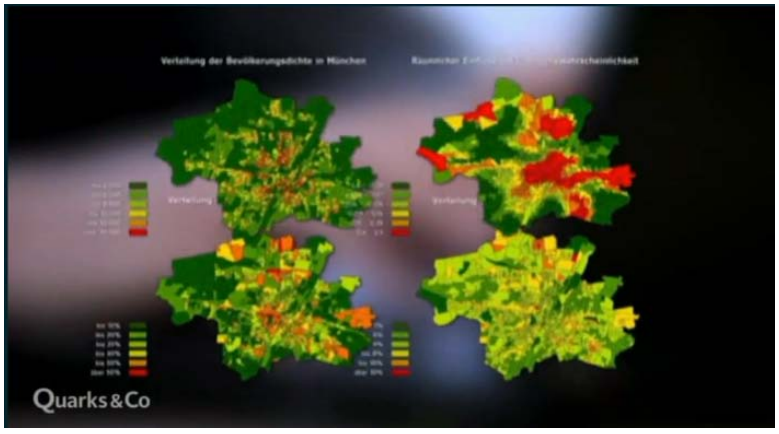

Figure 1. Merging different data sets for crime prediction (Quarks & Co, 2014).

On a national and international level public policy, law and regulation continually have to strive for politically defensible positions involving protection of individual rights and collective security (Ng-Kruelle et al., 2002; Perusco and Michael, 2007).

The EU research project CAPER (2014) will go one step further. It is planned to investigate all of us at an unprecedented scale. All available data

on the network of a person such as photos, videos, sounds, other files are planned to be tracked and evaluated by computers. The goal is to make impending crime of a person predictable in order to thwart them. Public surveillance cameras are used for screening unusual behaviour of passers-by. "We slowly recognise that science and technological progress at best can cause that more people can live a better life. However, this is achieved only for a certain time until new boundaries appear on which the same and in addition other problems arise that might even be bigger" (compare Sperry, 1983). At the moment streetlights are equipped with surveillance cameras. Hence it becomes very cheap and efficient to combat crime. In the future, it is likely that completely automated UAVs with cameras and location sensors including GNSS and inertial sensors (see Figure 2), can merge datasets, such as judicial rulings, police protocols and will be able to create movement profiles and can detect conspicuous behaviour of any suspicious person. Whereas electronic surveillance clearly was seen as an intrusion on personal freedom, today, many in the US would be willing to accept privacy restrictions and allow the government far "greater liberty to use surveillance technology to combat terrorism" (Olsen and Hansen 2001, cited in Ng-Kruelle et al., 2002).

Figure 2. Tiny UAV equipped with a camera and location sensors (RIANOVISTI, 2014).

5. Legislative and Political Activities

On the webpage of the German government commissioner for data protection and freedom of information, Schaar (2014) informs about using LBS but there is no regulation, law or ethical standard and guideline relevant for App developers, LBS researchers, providers or users. Schaar promotes that providers should comprehensively inform users of LBS in advance about which data is collected and how and to whom they are sent. The data protection law is a mandatory requirement for the transfer and use of location data with the subject's consent only. The users should have the possibility to

withdraw their consent at any time. Furthermore, the customers of LBS would be able to turn off the location temporarily or permanently. Schaar argued that "the consideration of data protection is in the interest of the seller. Without adequate protection the expected success of LBS will be denied". He pointed out that the European Directive on privacy and electronic Communication contains detailed rules concerning LBS that will be implemented in the ongoing revision of the Telecommunications Act in Germany. The data protection supervisory authorities will ensure that these requirements of the companies are respected. From the perspective of data protection, significant new risks may arise, said Schaar. There is a risk that data can be passed on to third parties including movement profiles, personal lifestyle and consumer behaviour. In this way data pools may arise that are no longer controllable (Quarks & Co, 2014).

In 1950 Article 8 para 1 of the European Convention on Human Rights ensures and claims for a person to respect his private life, his family life, etc. Several European countries included this article in paraphrases in their Basic Law. 1974, a resolution on the processing of personal data has been adopted as a non-binding appeal to the Member States. The EU's data protection rules, introduced in 1995, are outdated and need a comprehensive reform to strengthen individual rights and tackle the challenges of globalisation and new technologies. In 2010 a comprehensive survey was conducted on "Attitudes on Data Protection and Electronic Identity in the European Union". The results show that European Internet users feel responsible for handling their personal data but 90% would prefer equal protection rights across the EU and regulation should be introduced to prevent companies from using people's personal data without their knowledge. Such companies "should be fined (51%), banned from using such data in the future (40%), or compelled to compensate the victims (39%)" (European Commission, 2011). In March 2014 the EU Commission announced progress on the long awaited EU data protection reform. The EU Parliament voted for an upcoming regulation that will establish a single, pan-European law for data protection, replacing the current inconsistent patchwork of national laws (European Commission, 2014).

6. Conclusion

"We are moving into a world where your location is going to be known at all times by some electronic devices. [...] It's inevitable. So we should be talking about its consequences before it's too late", said Smarr in 2003, Funder of NCSA (National Center for Supercomputing Application) and now director of California Institute for Telecommunications and Information Tech-

nology. There is a lot of research and development going on in developing algorithms to keep ones data and search request in private. Questions arise like: How often is our research community thinking about values and ethical responsibilities? Are we aware of the social and ethical dimensions with regards to research activities and possible future implications? Already or in the near future does the lack of consciousness or failing to disclose ethical considerations have an effect on the credibility of LBS research? We are certain that a lot of us do think about ethics, norms and values but only few of us articulate and address this issue within their department, in public or when publishing research results. "The future of the exact sciences is highly dependent on whether or not the public in general is attesting them a competence in the realm of values" (Sperry 1983).

From the very beginning of the research process technical researchers, which are only working on the improvement of ubiquitous positioning to achieve a higher availability, integrity and reliability in any environment and more precise location determination, should include the issue of the user's privacy. Obviously it is not enough to develop new, innovative technologies and to take the lead. It is time to think not only in technical terms, but also its potential danger in our newly created knowledge. Moreover, the research results must have a positive impact on our society and the future.

In his Book "Who Owns the Future" Lanier (2013) argues: "This is what diverse cyber-enlightened business concerns and political groups all share in common, from Facebook to WikiLeaks. Eventually, they imagine, there will be no more secrets, no more barriers to access, all the world will be opened up as if the planet were transformed into a crystal ball. [...] The Problem Is Not the Technology but the Way We Think About Technology". In this regard we apparently cannot expect of the politics not only to surround itself with technical but also with social science and ethical advisors. For researchers and developers, this means that they have to self-regulate and set limits on their own. They need to scrutinize and control themselves. Ethical counseling at Technical Universities would be a first step in this direction, the implementation of an ethics committee the second.

An ethics committee does not mean to say no or forbid LBS research projects. This is not the implicit function of an ethics committee on University level. It will first discuss and consult research proposals amongst them and then provide a platform for a researcher or research team to examine the implications of the ethical impact of research projects and its possible research outcomes.

In social sciences it is mandatory that, ethical questions have to be considered and addressed, not only when conducting data collection but also for the ethical and moral impact of the expected results and consequences for its individuals, users or population. Over the past decade LBS developed very fast in many research directions. Hence, it becomes more and more influential in everyone's daily life privacy. Social scientists and scientists in the health sector have one advantage, when it comes to difficult questions with regards to ethical responsibilities and implications. They can or even must state their research proposal to an ethics committee. We think that it's time that no longer only medical and social science faculties have an ethics committee to support and counsel their researchers. We have shown that also on Technical Universities the integration of the dimensions like ethics, values, morals and political responsibility become a serious necessity to be included in their research and teaching activities.

And as a final conclusion the authors are claiming:

1. Privacy and data protection has to be openly and formally considered in every LBS research project from the very beginning.
2. Ethics and research ethics as a subject have to be taught at every Technical University.
3. Every Technical University has to implement an ethics committee or to cooperate with another (Technical) University that has a ne thics committee.
4. Privacy and data protection has to be part in every country's Basic Law and as academics we are responsible for promoting it.

References

Ahas R, Silm S, Järv O, Saluveer E, Tiru M (2010) Using Mobile Positioning Data to Model Locations Meaningful to Users of Mobile Phones. Journal of Urban Technology, 17(1): 3-27

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

CAPER (2014) Collaborataive Information Acquisition Processing Exploitation and Reporting for the Prevention of Organised Crime. http://www.fp7-caper.eu/. Accessed 6 June 2014

Damiani M L, Bertino E, Silvestri C. (2009) Protecting Location Privacy Against Spatial Inferences: the PROBE Approach. ACM SPRINGL '09, November 3, Seattle, WA, USA

European Commission (2011) Special Eurobarometer 359 – Attitudes on Data Protection and Electronic Identity in the European Union. Report. Fieldwork: November – December 2010. Publication: June 2011

European Commission (2014) Reform of Data Protection Legislation. http://ec.europa.eu/justice/data-protection/. Accessed 9 Ocotber 2014

Grejner-Brzezinska D A, Toth C (2013) GPS-challengend Environments – Can Collaborative Navigation Help? Proceedings of the 8th International Symposium on Mobile Mapping Technology, May 1-3, 2013, Tainan, Taiwan

Kalnis P, Ghinta G, Mouratidis K, Papadias D (2007) Preventing Location-based Identity Inference in Anonymous Spatial Queries. IEEE Transactions on Knowledge and Data Engineering. 19 (12): 1719–1733

Kealy A, Retscher G, Toth C, Grejner-Brzezinska D A (2014) Collaborative Positioning – Concepts and Approaches for More Robust Positioning. Proceedings of the XXV International FIG Congress, June 16-21, 2014, Kuala Lumpur, Malaysia

Kido H, Ynagisawa Y, Satho T (2005) Protection of Location Privacy using Dummies for Location-based Services. Proceedings of the 21st International Conference on Data Engeneering ICDE '05

Lanier J (2013) Who Owns the Future. Simon and Schuster, New York, USA

Mascetti S, Bettini C, Freni D, Sean Wang X (2007) Spatial Generalisation Algorithms for LBS Privacy Preservation. Journal of Location Based Services. 1(3): 179-207. Taylor & Francis, Bristol, PA, USA

Ng-Kruelle G, Swatman P A, Rebne D S, Hampe F (2002) The Price of Convenience: Privacy and Mobile Commerce. Quarterly Journal of Electronic Commerce, 3(3): 273-285

Olsen S, Hansen E (2001). Attacks Silence Privacy Concerns. News.com

Perusco L, Michael K (2007) Control, Trust, Privacy, and Security: Evaluating Location-Based Services. IEEE Technology and Society Magazine. Spring 2007

Quarks & Co (2014) Die Macht der Daten – The Power of Data. WDR German Television. http://www.ardmediathek.de/tv/Quarks-Co/Die-Macht-der-Daten/WDR-Fernsehen/Video?documentId=21546508&bcastId=7450356. Accessed 27 May 2014

RIANOVISTI (2014) Drone Market Set to Take off in U.S. http://en.ria.ru/business/20120913/175942371.html. Accessed 6 June 2014

Saluveer E, Ahas R (2010) Mobile Telephones and Mobile Positioning Data as Source for Population Statistics. Presentation at the European Forum for Geography and Statistics, Tallin, Estonia. http://www.efgs.info/workshops/efgs-2010-tallinn-estonia/efgs2010/29_Mobile_telephones%20and%20mobile%20positioning%20data%20as%20source%20

for%20population%20statistics_%20Erki%20Saluveer%20et%20al.pdf. Accessed 18 August 2014

Schaar P (2014) Data Protection – A European Basic Right. http://www.bfdi.bund.de/EN/EuropeanInternationalAffaires/Artikel/DataProtectionAEuropeanBasicRight.html?nn=408878. Accessed 6 June 2014

Schirrmacher F (2014) Die Macht der Daten – The Power of Data. WDR German Television. http://arscommunication.wordpress.com/2014/06/13/frank-schirrmacher-die-macht-der-daten/. Accessed 27 May 2014

Smarr L. (2003) http://lsmarr.calit2.net/index. Accessed 6 June 2014

Sperry R. (1983) Science and Moral Priority. Columbia University Press, New York, NY, USA