TRADING-OFF LOCATION OBFUSCATION AND QUALITY OF SERVICE: A WAY TO ENSURE PRIVACY?

Zoe Gardner
Nottingham Geospatial Institute, University of Nottingham, Nottingham, UK
Zoe.Gardner@nottingham.ac.uk

Didier Leibovici
Nottingham Geospatial Institute, University of Nottingham, Nottingham, UK
Didier.Leibovivi@nottingham.ac.uk

Anahid Basiri
Department of Geography and Environment, University of Southampton, Southampton, UK
A.Basiri@southampton.co.uk

Giles Foody
School of Geography , University of Nottingham, Nottingham, UK
Giles.Foody@nottingham.ac.uk

***Abstract*—Location privacy has become a growing concern impeding the adoption of many Location Based Services (LBS). Although there have been several approaches, such as anonymisation or obfuscation of location data, none has yet been completely successful at addressing privacy protection. This paper discusses the results of 256 survey responses which show that users' demands, expectations and concerns vary significantly among different user groups (by age, education, income, technological experience and social media activity) and infer that there is no 'one fit for all' solution for different LBS applications due to the variation in use.**

Keywords—Location Privacy; Location-Based Services (LBS); Demographic Information;

I. INTRODUCTION

Location Based Services (LBSs), such as navigational tools and location-aware advertising are services delivering mobile data and information where the contextual content to the user is tailored to the current or a projected users' location [1]. Personalisation is one of the key features of LBS and is welcomed by many users. Knowledge of a user's location enables LBSs to provide more specific services to the individual as personal preferences can co-analysed relevant to geo-located characteristics. However, personalisation also raises concerns regarding users' privacy particularly when including their location. Requiring personal preferences, history of activities and more importantly, current location and recent trajectories of movements, personalisation could disclose rich information to other parties [2]. Location awareness alone can reveal a lot about an individual, therefore, location privacy is one of the most concerning among wider privacy debates for the adoption of LBS applications [3, 4].

In order to access LBSs, mobile users are required to disclose their location to the service provider. This information can be subsequently be accessed by the same or other sectors without the user's permission. The availability of this data allows users' activities, preferences, health and identity to become characterisable, traceable and in some cases uniquely identifiable [5]. One study showed that 87% of mobile users can be uniquely identified, including their postcode, age and gender, using a collection of non-identity attributes [6]. A further study found that only four anonymous spatio-temporal points are enough to uniquely identify 95% of the crowd [7]. The potential to re-trace users' identities in this way has raised serious concerns due to potential privacy violations, positioning it as one of several obstacles to the adoption of LBS applications [8].

Privacy protection relies on the employment of several approaches and mechanisms [9]. These can be categorised as: (1) Regulatory approaches: the development of rules to govern the fair use of personal information and therefore certain guarantees of privacy [10]; (2) Privacy policies: trust-based mechanisms for prescribing certain uses of location information [11]. Their aim is to provide protection that is sufficiently flexible to be adapted to the individual user's requirements, situations and transactions [12]; (3) Anonymity: the dissociation of user information, including location, from an individual's identity [13]; (4) Obfuscation: the process of degrading the quality of information about a person's location, with the aim of protecting user privacy [14, 15]. Each of these approaches has its own challenges and limitations and so many applications use a combination to protect privacy [16].

As one of the four approaches to protect location privacy, *i.e.* (a) regulatory, (b) privacy policies, (c) anonymity and (d) obfuscation, the fourth, *obfuscation* adds uncertainty to the location information (position and its accuracy). This introduces inaccuracy, vagueness, incompleteness, inconsistency, and imprecision in order to lower the associations between positional data and reality. Although obfuscation can protect the privacy of users in many scenarios, it can be viewed as a challenge to the quality of LBS responses requested by users, i.e. lowering the quality of the position lowers the quality of returned service. This loss of

quality of service can vary with respect to the type of application; for example in pedestrian navigation services, the impact of inaccuracy and imprecision on the quality of the final service can be significant. While for Location Based Social Networking (LBSN), vagueness in input data, *i.e.* using vague/fuzzy spatial concepts such as 'near', 'around', 'close to' instead of the actual coordinate, may still provide an acceptable level of service.

The goals of this paper are: (1) to examine the extent to which privacy is a concern for users and whether factors such as age and education can predict attitudes towards privacy; and (2) to establish to what extent users are happy to compromise service quality (and therefore optimum uncertainty) levels to protect location privacy. Policies and regulations would then allow the application to have access to a user's location with a controlled level of accuracy, either automatically or manually, assuring a desired level of location privacy. Giving the user more options to share/disclose their position with different levels of accuracy and continuity may attract those who have declined, for privacy concerns, to use the LBS applications and services.

The second section of this paper reviews current privacy protection approaches and evaluates their challenges and limitations. Various location obfuscation mechanisms are examined. Typical scenarios and contexts illustrating when such compromises are made are considered. This leads to the third section which outlines the hypothesis and research questions. Section four describes the methodology and survey results which address the research questions. The final section dedicated to discussion, conclusion and future work.

II. LOCATION PRIVACY CONCERNS AND POSSIBLE SOLUTIONS

A. Location Privacy Protection Approaches

The threats associated with the violation of location privacy can dramatically limit the development, adoption and growth of LBS applications. LBS require users to disclose their locations in order to access more relevant and personalised services. LBS providers can potentially store, (mis-/re-) use, and even sell location data. Such potential threats to privacy can discourage users sharing their location [17]. Additionally, a sequence of a user's locations can potentially disclose activities, preferences, health, background, history and many other personal aspects. When the sequence of locations is time stamped, *i.e.* knowledge of the movement trajectory, greater levels of detail can be revealed [18], with up to a 95% chance of uniquely identifying a person with only four spatio-temporal points [7].

If these privacy issues are already well understood, the lack of awareness regarding location privacy among ordinary LBS users may in fact be damaging for LBS providers given the potential for users to overestimate the potential threats [17, 19]. This is partially due to the fact that each application and service does not necessarily require the same level of accuracy relevant for a service, while positioning solutions are not provided with the minimum required level of accuracy. Therefore, the access or inference of higher-level private information and the potential impact of privacy violation in each LBS application differs [20]. Minimum required levels of accuracy, continuity and availability of location data for LBS application clusters entailing a potential threat to the privacy are discussed in [16].

Privacy concerns over location awareness have introduced major challenges to mobile applications and services, including LBSs. Blockage or denial of location sharing, has introduced a major challenge to the provision of personalised LBSs and the development of the LBS market in general. Studies have shown that up to 72% of smartphone owners in the US and 68% in Europe change the location settings of their smartphones to disable location sharing. More than 95% of the time, this is done regardless of the type of application/service, some of which can be life-saving/changing. However, recent research has found that location privacy concerns could depend on the type of application [20].

There are currently four approaches to location privacy protection, of which have their own challenges [8]: Regulatory, privacy protection, anonymity and obfuscation. The regulatory approach, developed by governmental and legislative sectors to define rules to manage privacy have faced several challenges. In particular, the numerous ways in which they can be interpreted and therefore implemented [15]. In addition, due to the time-consuming and complicated process of rule and legislation development, the number of privacy regulations is relatively small [8]. Regulations on their own, cannot guarantee or even prevent the invasion of privacy as they are only employed when the privacy violation occurs. The regulations and rules can only exist to ensure the accountability of governments and subsequent enforcements in the case of privacy invasion. Nonetheless, we could imagine the development of labels, such as ''in agreement with privacy regulation n°'' for LBSs, so that users would be informed when installing applications.

While regulatory approaches target the global or group-based safeguards, *privacy protection* approaches provide more flexible and adaptive protection mechanisms to facilitate use by individuals [21, 22]. The Internet Engineering Task Force (IETF), GeoPrive, the World Wide Web Consortium (W3C)'s privacy preferences project (P3P) and Personal Digital Rights Management (PDRM) are of the most active bodies in developing privacy standards for policies in LBSs. However, adoption of these policies has proven to be slow due to the nature of LBSs. The fast growing, highly innovative ecosystem of LBSs, which follows the trend in new technologies, makes it difficult for the policies to be adopted to protect the newly encountered situations. This challenge, shared by the regulatory approaches, becomes even more problematic when the privacy policies need to rely on the available regulation to be practically applicable.

Anonymity provides a mechanism to minimise traceability of the information and the individual's identification with other

associated data. The anonymity-based approaches, such as *k*-Anonymity [23], disassociate the location information from the user's identity or minimise the possibility of inference and traceability to the user's non-identity information (i.e. at least *k* users would satisfy the inferential system, not less). Although the *k*-anonymity approach is technically easy to apply and implement, it can be viewed as a barrier to the personalisation features of LBS, increasingly popular and essential for many applications [24]. A possible solution might be pseudonymity-based approaches as they partially allow some levels of personalisation. These approaches keep the individual's real identity anonymous while giving a persistent pseudonym. Therefore the privacy is protected by using an alias, which can be potentially linked with their actual identity under higher safeguards. Although pseudonymity could be an answer to the problem of personalisation, the sequence of pseudonymised locations may lead to the identification of the individual if this sequential data is also added to other non-identical data. Reference [6] showed that 87% of users can be uniquely identified using a collection of non-identity attributes, including postcode, age and gender.

The fourth category is *obfuscation*. Obfuscation lowers the positional accuracy of a user's location to prevent its mis/re-use [9]. In doing so, obfuscation reduces the possibility of associations between positional data and specified real information, playing with the existence and boundaries of data [8].

Although obfuscation can protect the privacy of users in many scenarios, it brings a challenge to the quality of LBS provision. The quality of service provided by LBS applications highly depends on the quality of available positional data. This correlation depends on the application type. While anonymity hides an individual's identity and its associations with location, obfuscation, which degrades the spatial quality of the data, allows the individual's identity to be revealed and be 'vaguely' associated spatially. A disadvantage of obfuscation therefore, is the potential to match other datasets and thus obtain a more accurate location and reveal more about the user, to the point of contradicting the level of disclosure in the location setup during installation.

A. Location Obfuscation

The location of the user is given by an estimate of geographical coordinates, a position, and a measure of the accuracy of this position. For example, an Android device will give a GPS coordinate with a 68% circular error (radius corresponding to 1 standard deviation), giving a 'halo' or area where the user is located. Reference [25] defined obfuscation of the location as something that is obtained after a series of transformations, either on the position estimate, 'shifting the position' or on the accuracy measure 'enlarging artificially the accuracy radius'. The obfuscation level can be measured by comparing the final accuracy to the best possible option [25, 26].

As one of the four approaches to protect location privacy, *obfuscation* adds uncertainty to a users' location information (positional accuracy) by introducing inaccuracy, vagueness, incompleteness, inconsistency, and imprecision in order to lower the associations between positional data and reality. Although obfuscation can protect the privacy of users in many scenarios, it can be viewed as a challenge to the quality of LBS responses requested by users, i.e. lowering the quality of the position lowers the quality of returned service. This loss of quality of service can vary with respect to the type of application; for example in pedestrian navigation services, the impact of inaccuracy and imprecision on the quality of the final service can be significant. While for Location Based Social Networking (LBSN), vagueness in input data, *i.e.* using vague/fuzzy spatial concepts such as 'near', 'around', 'close to' instead of the actual coordinate, may still provide an acceptable level of service.

In this scenario, a novel contribution of the paper is represented by a comprehensive solution aimed at preserving location privacy of individuals through artificial perturbations of location information collected by sensing technology. In particular, location information of users is managed by a trusted middleware [5,6,9], which enforces users privacy through obfuscation-based techniques.

Key to this work is the concept of relevance as the a-dimensional metric for the location accuracy. A relevance value is always associated with locations and it quantitatively characterizes the degree of privacy artificially introduced into a location measurement. Based on relevance, it is possible to strike a balance between the need of service providers, requiring a certain level of location accuracy, and the need of users, asking to minimize the disclosure of personal location information. Both needs can be expressed as relevances and either quality of online services or location privacy can be adjusted, negotiated or specified as contractual terms.

III. SURVEY AND RESPONSES

The survey focused on the levels of different aspects of spatial uncertainty, including inaccuracy, vagueness, incompleteness, inconsistency, and imprecision [s] required to provide acceptable levels of service quality whilst preserving the privacy of users for navigation services (as the largest revenue generator segment of LBS). The aim is to identify the optimum framework for modelling spatial uncertainty for the purpose of *obfuscation* of location data in location privacy protection. The research questions concern the trade-off between the desired quality of service expected and levels of privacy protection derived from the levels of obfuscation.

A first set of questions aimed to assess the views and perceptions of users' location privacy. These were then correlated with users' profile data relating to age, gender, educational attainment and activity profiles (social media and navigational services activity).

A. Survey Structure and Participants Demographics

In February 2017 a survey was conducted to explore the extent to which user's were prepared to compromise location privacy for quality of LBS. A sample of 239 *SurveyMonkey*

participants were surveyed. Participants were represented by an approximate female to male ratio of 2:1 (60.7% female, 38.5% male and 2.38% other). With regard to age, 15% of respondents were below 30, 83% 20 or over, 56.5% 50 and over, thereby representing mainly the views of this age cohort.

With regard to educational attainment, 35.5% did not hold a first degree, whilst 38% had a first degree and 26.5% a postgraduate qualification (Masters or PhD). This suggests a reasonably even representation of education levels.

B. Survey Results

Privacy concerns. The research aimed to assess the extent to which users were prepared to compromise their location privacy for an improved quality (accuracy) of LBS (knowing that the quality of the output service could be compromised if they increased the levels of location privacy). The research hypothesised that given the choice users are more likely to choose not to degrade the quality of positioning.

Respondents indicated if and why they change the location settings of their mobile devices due to privacy concerns. Participants were offered 5 different responses or the option to provide their own reason. These options included "They can track me (even if I am not using a navigation service)", "My data can be given to individuals without my permission", "My data can be sold to a third party without my permission", "My data can be reused by the same service provider for other purposes (such as advertisement)", and "The apps/services I use do not seem to need my location". Respondents were asked to provide the significance of their decisions based on a 5-point scale, ranging from "very important" to "completely irrelevant". Reliability of the three items was high, $\alpha = 0.84$, 0.83, and 0.88 for navigation services, Location-Based Social Media, and Advertisement and deals, respectively. On aggregate 49% of respondents were prepared to trade-off location privacy in order to retain LBS quality, in terms of individual trajectories and traceability. However, 15% of respondents were willing to trade-off quality of service for location privacy in terms of traceability. When the prospect of data sharing (between third parties/re-used by the provider) was introduced, the extent to which users were prepared to trade-off location privacy for service quality was reduced to around 30%, with on average 30% of users prepared to compromise service quality completely for location privacy protection.

Location obfuscation. Users' privacy concerns were supported by more specific questions regarding location obfuscation. Participants were asked for which scenarios they would be prepared to degrade their location data that was disclosed to an app/service provider in order to protect location privacy. In this part of the survey the participants were briefed that some quality aspects of the final service, such as availability or accuracy of the navigational instructions or frequency of traffic data updates, would be compromised. Based on several scenarios respondents were then asked to select what level they would like to degrade their input position knowing the output navigation service would be less reliable or accurate, by selecting how likely they would be to select this scenario. Respondents had three options of "very likely", "maybe", and "very unlikely". Then they were asked to state the optimum balance, from their point of view, for the proposed scenarios.

Overall, 46% of respondents said they were "very likely" to disclose their location information for the best quality of service for journey planning, i.e. not obfuscate their location data at all. While 17% of respondents responded that they would be "very unlikely" to do this. When presented with the option to obfuscate their location to within 1km accuracy and receive service updates every minutes (the highest degree of obfuscation/lowest quality option given) these figures were almost revered, with 47% of respondents stating that they were "very unlikely" to do this and 21% stating that they would be "likely" to opt for this scenario. The most acceptable levels of obfuscation sat somewhere between 100-200m locational accuracy for accurate service updates every 2-3 minutes, with 72 of participants responding with "very likely" or "maybe" to these two scenarios.

When asked whether respondents would be willing to share their location whilst not using a navigational LBS, over 83% stated that they would either be unwilling to do this (61.3%) or would want the option to interrupt this feature if required (22%). Thereby suggesting data sharing with no advantages (i.e. service provision) is overwhelmingly unacceptable to users.

Privacy concerns and user profile interactions. The second part of the research aimed to look at whether there is an interaction with age, education and activity levels on social media or use of navigation apps? Frequent navigation service/app users show more likelihood of sharing:

Some results on this are required here:

IV. DISCUSSION, CONCLUSION AND FUTURE WORK

With the growth of social media as a platform to share photos, feelings, plans and news (particularly among the younger generation) a reasonable assumption was made that, due to frequency of posting, active users of social media are less concerned about general privacy. Therefore, for active social media users, the research attempted to ascertain the correlation between degrees of privacy concerns and levels of activity. Extreme views on location privacy, *i.e*. no concern at all and no disclosure could be linked to various factors including educational attainment or technological knowledge. Some studies (references) support the hypothesis that lack of education and/or technological awareness (often highly correlated with age) are associated with ignorance regarding privacy and risks associated with disclosed location. However, it has also been found that there is an exaggeration or overestimation in the threats of disclosing user related data (references). For location data and associated privacy concerns, this could be different as location and movement data can tell a lot about an individual and so the potential threats might be higher, or less appreciated or simply ignored

due to a lack of education or lower age. So an important question is about the relations between age, education level and the location privacy concerns expressed.

A Correspondence Analysis of the contingency table crossing the Research questions (Q8-Q13) and descriptors of the profiles of the respondents has been performed (see Leibovici DG, and Birkin MH (2013) Simple, multiple and multiway correspondence analysis applied to spatial census-based population microsimulation studies using R. This multidimensional analysis act as a dimension reduction like PCA (Principal Component Analysis) but also offers a break-down decomposition of the distance to independence measured by the chi-square statistic on this contingency table (generalising a chi-square measure between two categorical variables), so describing the lack of independence between the answers to Q8-Q13 and the characteristics of the respondents: socio-demographic descriptors and attitudes towards using social media and navigation apps. Associations within the categories of these descriptors used (e.g. male and oldest) with questions responses (e.g. would not disclose location for better service (from Q11) and high privacy concerns because of tracking (fromQ8)) are depicted from the pairs of components associating the rows and columns for each dimension captured. The analysis of the 26 x 80 table (see variables involved in the results) explain for the three best dimensions 29%, 16% and 11% of the lack of independence, so capturing non-expected associations under the hypothesis of independence.

To facilitate the interpretations and reading the associations between rows and columns, each dimension has been summarised in Figure 1. The coordinates on the components are ordered from positive to negative values. The *ctr* and *cos2* statistics are used to retain what is significant in giving a meaning to the captured dimension, *i.e*. looking for associations (same side of the dimension), or oppositions (opposite sides of the dimensions). The *ctr* (standardised to 1000) expresses how the variables contribute to the dimension inertia, e.g. the 29% of the total inertia that is captured by dimension dim1. So, across the rows or across the columns the sum of the *ctrs* are 1000 and for example 148/1000 or 14.8% of these 29% are due to '0.Navapp' answers (not using any navigational app). The *ctr* values have to be compared to the average *ctr*, for example the column variable 'Q12.TradeOff.Scen.200.coar.likely' contributes to 44 out of 1000 of the semantic of the component which is nearly 4 times the average contribution of 12.5 out of 1000 (as 1000/80=12.5). In each table only column variables that have a *ctr* greater than 12.5 are displayed. For the rows 'monthly.Nav ' is contributing to 89 out of 1000 on the negative side of the axe; the average contribution is 1000/26=38.5, but we displayed all rows in the figures. The *Cos2* expresses how well, in a regression sense, the variable is explained by the dimension (as projected on this dimension); therefore, the sum of the *Cos2*s across the dimensions equal 1000. It can be interpreted as an R^2. Therefore, for a variable (row or column) to be able to bring its semantic into a dimension needs to contribute enough (ctr) and to be relatively well explained by this dimension as well. The number of stars put in the figures 1-3 are highlighting the variables useful to interpret the dimensions and so associations and oppositions within rows or columns and between them.

Active social media users (active on two or more applications) or those using a navigation service on a daily basis, who are less than 30 years old and sometimes change their location settings, are in opposition to non-active users of social media or navigation service or having no specific navigational service who are more likely to be older (over 50 year old) and regularly changing the location setting. The results show that gender and educational attainment do not play a significant role for dimension 1 (low ctrs) . This user profile is associated with the column component of dimension 1: 'likely' vs 'unlikely' concerning various tradeoffs between better service levels (Q10 and Q12) as well as an opposition to privacy concerns (Q8) linked also to disclosure control (Q11). Notice that the (young) frequent users of social media and navigation are at the same time considering the privacy concerns seriously (Q8 Important but Ok for No permission) and are likely to will to control the way the location and accuracy of service delivered but the rare users more likely older are not willing to compromise or disclose their location at all if they can.

In Figure 2, opposition between young female social media users changing their location settings (always or sometimes), and, male navigational app users (2 apps) who rarely or never change change the location settings with a tendency to be older and more educated (but ctr below average). The female profile is associated with willing to disclose location (Q11, Q13, Q12, Q9) but all with a very coarse resolution (accuracy). They also have a high concern about privacy to the point of not using the service in a tracking situation (Q8) as well as for the other situations in a lesser extent (here they have all above average *ctr*). This is opposed to Q8 privacy concerns situations judged as 'low impact but ok' or 'not concerned' (tracking) and share all the time the location (Q9) for the different Q9 tradeoff scenarios.

In Figure 3, the row variables component opposes navigational users who rarely change their location settings but who do not use social media apps and have a school level of achievement less than a degree, to users with a degree using on weekly basis a navigational app as well as social media and never change their location settings. The latter profile is in association with the column variables component highlighting a 'maybe' attitude on tradeoff between location disclosure and service accuracy (Q12) but who considering privacy is important nonetheless accepting to disclose it. For the former profile not using social media they prepared to disclose if promotions (Q11) or do not feel concerned or want best

service (Q13) but in the meantime point out to ‘likely’ for Q10 with quite coarse resolution (up to 10mn).

ACKNOWLEDGMENTS

The joint authors would like to acknowledge the assistance of Dr Christian Brignell, Dr Christian Wagner and Dr Andrew Wood in the development of the survey.

REFERENCES

[1] Brimicombe A. and Li C. (2009), LBS and GeoInformation Engineering. John Wiley & Sons publisher. ISSBN 978-0-470-85737-3.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[2] Toch E., Yang Wang, Lorrie Faith Cranor, “Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems”, User Modeling and User-Adapted Interaction, Springer Publishing, pp. 203-220 Doi: 10.1007/s11257-011-9110-z, 2012K. Elissa, “Title of paper if known,” unpublished.

[3] Basiri, A., Moore, T., & Hill, C. Bhatia, P. (2015a). Challenges of Location-Based Services Market Analysis: Current Market Description, Progress in Location-Based Services 2014, 273-282, Springer Publishing.

[4] Raij, A., Ghosh, A., Kumar, S., & Srivastava, M. (2011, May). Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 11-20). ACM.

[5] Premarathne, U. S., Han, F., Liu, H., & Khalil, I. (2015). Impact of privacy issues on user behavioural acceptance of personalized mhealth services. In Mobile Health (pp. 1089-1109). Springer International Publishing.

[6] Sweeney L., “K-anonymity: A model for protecting privacy”, International Journal of Uncertainty, Fuzziness and Knowledge-based Systems, 10(5): 557-570, 2002.

[17] Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. In Proceedings of the Eighth Symposium on Usable Privacy and Security (p. 1). ACM

[18] Chen, R., Fung, B. C., Mohammed, N., Desai, B. C., & Wang, K. (2013). Privacy-preserving trajectory data publishing by local suppression. Information Sciences, 231, 83-97

[19] Shokri, R. (2015). Quantifying and protecting location privacy. it-Information Technology, 57(4), 257-263.

[20] Puttaswamy, K. P., Wang, S., Steinbauer, T., Agrawal, D., El Abbadi, A., Kruegel, C., & Zhao, B. Y. (2014). Preserving location privacy in geosocial applications. Mobile Computing, IEEE Transactions on, 13(1), 159-173.

[21] Landau, S. (2015). Control use of data to protect privacy. Science, 347(6221), 504-506.

[22] Gorlach, W. W., Terpstra A., and A. Heinemann. Survey on location privacy in pervasive computing. In Proc. First Workshop on Security

[7] De Montjoye, Y. A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013). Unique in the crowd: The privacybounds of human mobility. Scientific reports, 3.

[8] Wernke, M., Skvortsov, P., Dürr, F., & Rothermel, K. (2014). A classification of location privacy attacks and approaches. Personal and Ubiquitous Computing, 18(1), 163-175.

[9] Duckham, M., & Kulik, L. (2006). Location privacy and location-aware computing. Dynamic & mobile GIS: investigating change in space and time, 3, 35-51.

[10] Quinn, K. (2016). Why We Share: A Uses and Gratifications Approach to Privacy Regulation in Social Media Use. Journal of Broadcasting & Electronic Media, 60(1), 61-86.

[11] Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B. G., Cox, L. P., ... & Sheth, A. N. (2014). TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. ACM Transactions on Computer Systems (TOCS), 32(2), 5.

[12] Myles, G., A. Friday, and N. Davies. Preserving privacy in environments with location-based applications. Pervasive Computing, 2(1):56–64, 2003.

[13] Pan, X., Xu, J., & Meng, X. (2012). Protecting location privacy against location-dependent attacks in mobile services. Knowledge and Data Engineering, IEEE Transactions on, 24(8), 1506-1519.

[14] Duckham M., and L. Kulik. A formal model of obfuscation and negotiation for location privacy. In H. W. Gellersen, R. Want, and A. Schmidt, editors, Pervasive 2005 , volume 3468 of Lecture Notes in Computer Science , pages 152–170. Springer, Berlin, 2005.

[15] M. Duckham and L. Kulik. Simulation of obfuscation and negotiation for location privacy. In D.M. Mark and A.G. Cohn, editors, COSIT 2005 , volume 3693 of Lecture Notes in Computer Science , pages 31–48. Springer, Berlin, 2005.

[16] Basiri, Anahid, Elena Simona Lohan, Terry Moore, Adam Winstanley, Pekka Peltola, Chris Hill, Pouria Amirian, and Pedro Figueiredo e Silva. "Indoor location based services challenges, requirements and usability of current solutions." Computer Science Review (2017).

and Privacy at the Conference on Pervasive Computing (SPPC), 2004.

[23] Niu, B., Li, Q., Zhu, X., Cao, G., & Li, H. (2014). Achieving k-anonymity in privacy-aware location-based services. In INFOCOM, 2014 Proceedings IEEE (pp. 754-762). IEEE

[24] Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. Decision Support Systems, 51(1), 42-52.

[25] Ardagna et al (2007)

[26] Andrés et al. 2013

[27] (Worboys, 1998),

[28] Basiri, A., Moore, T., Hill, C., & Bhatia, P. (2016). The non-technical challenges of Location Based Services markets: Are the users' concerns being ignored?. In Localization and GNSS (ICL-GNSS), 2016 International Conference on (pp. 1-5). IEEE