Searching for Temporal Dependencies in the Privacy Concerns of Location-Based Service Users

Antonios Karatzoglou

Karlsruhe Institute of Technology
and Robert Bosch,
Corporate Sector Research
and Advance Engineering
Germany
Email: antonios.karatzoglou@kit.edu
antonios.karatzoglou@de.bosch.com

Julia Anken,
Florian Banscher,
Lukas Diewald

Karlsruhe Institute of Technology
Germany
Email: {julia.anken,
florian.banscher,
lukas.diewald}
@student.kit.edu

Michael Beigl

Karlsruhe Institute of Technology
Pervasive Computing Systems
Germany
Email: michael.beigl@kit.edu

***Abstract*—As the number of Location-Based Service (LBS) users grows steadily worldwide, the need for data protection and privacy-respecting methods and standards grows with it. There exists a big variety of privacy enhancing approaches by now. However, very few seem to have explored the impact of time on people's sense of privacy. In this work, we attempt to answer the question whether and to what degree privacy concerns with respect to location sharing are time-dependent or not. For this purpose, we designed and carried out 2 different user studies, a Web survey and a 4-week long experimental study. Our analysis shows evidence towards an existing dependency between time and the users' willingness to share their location. Moreover, the effect appears to be highly user-specific and correlates with certain personal features, such as conviviality and the general personal view on privacy and data protection.**

***Keywords*—Data protection and Privacy; Location Based Services; Semantic Trajectories and Locations.**

I. Introduction

In recent years, mobile service providers rely increasingly on context and in particular on location awareness in order to raise the quality of their service. As a result, the number of Location-Based Service (LBS) users has experienced enormous growth worldwide. Only in the US, it has been doubled in the last 5 years and expected to reach 242 million in 2018 [1]. Location-Based Services go nowadays beyond the sole knowledge of the coordinates of some single point on a map, e.g., for navigation purposes. Moreover, they make use of additional knowledge about the location, such as its type, corresponding activities and its opening hours, in order to be able to provide targeted recommendations to the users. In this case, this kind of semantically enriched locations may be referred to as *semantic locations* and the corresponding trajectories as *semantic trajectories* [2]. Semantic trajectories support an application-oriented and thus a more sophisticated way for modeling, analyzing and predicting human movement patterns like in [3]–[6]. Since most modeling approaches are data-driven, a large amount of tracking data is necessary in order to achieve a good performance. However, large high-quality datasets are hard to find. Rising privacy concerns and strict privacy guidelines further aggravate this problem. Two recent reports underpin this fact and show that almost half of teen and over a third of adult smartphone app users have turned off the location tracking feature at some time on their phones or tablets because they worried about who might access their data, [7] and [8].

Due to this fact and due to privacy becoming a generally very important issue of our data-overflowing society, many developers and researchers lay their focus on finding new methods to protect the privacy of LBS, and not only, users. This led to the emergence of so called *Privacy Enhancing Technologies (PET)* [9] and *Privacy by design* approaches [10]. These aim at taking human values and privacy explicitly into account and incorporating them into the development process of services, while at the same time acting in accordance with the data protection laws. There exists a great variety of different approaches and ideas behind these methods. In the location and tracking scene, current works base primarily on spatial obfuscation techniques, such as GPS grid masking [11] and spatial cloaking [12] to name but a few. According to these techniques, certain location types or spatial areas that are considered to be sensitive, such as hospitals, are being *obfuscated* either by reducing the spatial resolution or by anonymizing single individuals behind a bigger group of people.

However, the aforementioned methods are static and despite the dynamic nature of human behaviour none seems to have investigated the impact of time on the users' privacy concerns so far. In the presented work, we attempt to explore whether and to what degree time affects the users' sensitivity when it comes to providing information about their location. In other words, we want to find out if there exist situations, in which a user experiences a certain location sometimes more and sometimes less critical in terms of revealing the particular location. For instance, a visit to a bar in the evening might

ISBN: 978-1-61208-676-7

for some users be alright to share, whereas a visit to the same bar in the morning not, especially when social standards and values are taken into account. Adapting to this kind of potential temporal privacy concerns would make location-based applications more trustworthy and user-friendly. In order to explore such temporal effects, we conducted and evaluated 2 user studies, an online survey and a 4-week long experimental study. During both studies, the participants were asked to provide information about their willingness to reveal their location together with a brief explanation.

The rest of this work is structured as follows. In Section II, we provide a brief overview on some of the most related work in the field of privacy and privacy protection. Sections III and IV describe in their first parts the details of our two user studies. Their second parts include our evaluation results and interpretations. Finally, in Section V, we summarize our work and provide some concluding thoughts.

II. Related Work

The first part of this section provides insight into some basic work in the theory of privacy and privacy protection. The second part gives a short overview of location protection related work used in Location-Based Services.

A. Privacy Theories

A big variety of privacy theories has been developed so far. Here, we discuss two of these theories, which have been most frequently applied over time and verified by diverse studies: the privacy theory by Westin and the privacy regulation theory by Altman [13].

The privacy theory by Westin was developed in 1967 [14]. In his work, Westin regards privacy as

> *the claim of individuals or groups, to determine for themselves when, how and to what extend information about them is passed on to others.*

When privacy is viewed in the context of social interaction, Westin describes it as

> *the wilful and temporary withdrawal of a person from the general society.*

His theory supports the existence of different levels of privacy that can be determined based on the following four states (or dimensions) of privacy: *Solitude, Intimacy, Anonymity* and *Reserve* and their corresponding degree of achievement. In addition, Westin found in [15] that the driving factors behind privacy attitudes depend on the one hand on the individual's level of distrust in companies or institutions and on the other hand on her fears of technology abuse, a fact that applies very well to our LBS use case. Westin's fundamental work led to the development of scales for measuring privacy such as the Marshall dimensions of privacy preferences described in [16].

Altman's privacy regulation theory [17] extends and refines in part Westin's work. In Altman's view, privacy is a dynamic rather than a static interaction withdrawal process, in which individual people (or groups of people) selectively control the access to themselves. In particular, his theory takes into account that people may open themselves to others at a certain time and close themselves off at another time. Thus, people's desired privacy level changes over time, a fact that can be attributed to different external or internal factors. Altman further describes an optimization process with two ends and an optimal interaction level somewhere in the middle. On the one hand, there is the end with too much interaction and on the other hand, the end with too little interaction. Both ends are considered to be unsatisfactory. The ideal privacy level, i.e., the optimal level of interaction lies in-between, can change over time and is different for each person. Finally, Altman's theory considers a set of behavioural mechanisms that can serve to achieve the desired level of social interaction and thus, of privacy. Verbal, para-verbal and non-verbal behaviour, as well as, similar to Westin's work, physical (territorial) distance and isolation from the rest represent some of them.

Westin's and Altman's work has been often applied and adapted respectively to match the requirements of our technocratic society, in which the physical world merges increasingly with the virtual one. Work, such as in [18] and [19], extend privacy by adding the notion of roles and boundaries in the virtual space and defining in this way virtual territories.

B. Privacy Protection Methods for Location-Based Services and Applications

Due to location being a strong personal identifier, privacy protection methods are an essential part of LBS. The location history of LBS users reveals loads of private and sensitive information about the user, which in turn may be used to provide deep insights into their personal lives, their identity, as well as into their personality and character. This makes location data particularly critical. Therefore, their protection is of great importance. There exist various location protective approaches. *k-anonymity* and *l-diversity*, represent two of them and are briefly introduced below.

k-Anonymity is a so called spatial *cloaking* technique. It builds up a coarse, *cloaked* area over the location of a single LBS user and enlarges it until $k-1$ other persons (users) are included in it [12] [20]. By doing so, the LBS provider or an attacker cannot distinguish an individual entry of a single user from at least $k-1$ other entries in the cloaked area and thus the single user remains unidentifiable. It is self-evident that the value of k plays a significant role in the performance of k-Anonymity.

The so called Feeling-based Privacy model of Xu et al. relies on the k-Anonymity method and considers privacy and its protection as a feeling of the user [21]. For this reason, it is difficult to find a practicable value for k and thus to reduce the feeling of the individual user to a numerical value. In the Feeling-based Privacy model, a user is able to set indirectly his desired anonymity level by defining spatial areas in which he generally feels secure and comfortable, the so-called *public* regions. The entropy of the selected areas is used to describe their popularity, which in turn is used as the anonymity level for subsequent requests to the LBS, and must be guaranteed to the user. The result is a more personalized version of k-Anonymity. However, both approaches wouldn't work if the $k-1$ other users were in a group, that is, if the corresponding $k-1$ (user-ID, location)-tuples contain same sensitive values as, for example, the same exact location. In this case, the cloaked area would be small and might fall inside a large critical location such as a hospital area. This would allow an attacker to still know the whereabouts of a user.

l-Diversity was introduced to solve this problem [20] [22]. This method extends the k-Anonymity approach by ensuring that the (user-ID, location)-tuples of a certain cloaked area contain at least $l-1$ different location types. This leads to a further enlargement of the cloaked area until it covers $l-1$ different locations.

In the aforementioned methods, the exact position is abstracted by including other users or different locations into the region of interest. This makes it difficult for LBS providers or an attacker to gather private and sensitive information and draw conclusions upon it. However, semantic information about the $k-1$ included locations can still become problematic for both models. For example, it is imaginable that a cloaked area contains only semantically similar places. In this case, it would be possible for an attacker to assign a semantic meaning to the whole area. This could be for instance the case if the cloaked area consisted solely of health service places, such as hospitals or medical specialists. An attacker could conclude that users from this cloaked area have either health problems or know people that have health problems or work in the health service domain. Similarly, if the cloaked area referred to a university campus, an attacker could conclude that the users are either students or belong to the academic staff. Although personal information is being revealed in both cases, the first (hospital) case is regarded as a more critical piece of information. Thus, locations show a different degree of sensitivity depending on their type. For this reason, recent approaches aim at protecting the semantics, that is, the meaning of locations as well, such as in Damiani et al.'s framework [23]. Lee et al. present in their work also such a *semantic cloaking* method, where cloaked areas are built up based solely on *different* semantic location types [20].

Finally, in [24], Marconi et al. extend the core idea of Xu et al. by interpreting feelings as dynamic, time-varying features. In their work, they define and evaluate new attacker models that have additional access to temporal information, such as the distribution of anonymized entries over the day. It could be shown that as soon as the factor time is included in the attacker models, the privacy protection assumed in the Feeling-based Privacy model could not be maintained. Moreover, their work is in line with our assumption that when it comes to privacy, time plays a major role. In contrast to the presented work, both Marconi et al. and Xu et al. evaluate their work on synthetic data and their focus lies primarily on the optimization of depersonalization servers.

III. User Study I

A. Overview - Description

Our first study included two parts. The first part aimed at establishing possible connections between demographic as well as personality characteristics and the sense of privacy among the participants. In the second part, we focused on learning more about the use of LBS running on smartphones with respect to privacy and willingness to share their location. For this purpose, we confronted the participants with the question whether they believe that the sense of privacy is time-dependent in various contexts. The goal was to identify the circumstances, with respect to time, under which, people would most likely reveal their data. In addition, the obtained data of this first study served also an additional purpose, namely as basis for the design and the content of our app in the main, experimental study described in the following Section IV. That is, we used the gained data in order to modify the app accordingly and be able to provide our participants with a high usability. This is particularly important when conducting a long user study, because users tend to close or remove apps with low usability more often.

For the purpose of our first study, we used the Google Forms online survey platform [25]. We asked a total of 52 people, which we recruited via email. Approximately three fourths of the participants were 18-25 years, with most being in education (e.g., college or university students or trainees). The rest of the participants were uniformly distributed within the range of 25-65 years old. In addition, three fourths were male and about 80% show a strong to very strong affinity for technology.

B. Evaluation

Due to the limited space, in this section we will focus on the most interesting findings. Figure 1 shows an interesting but also expected trend with regard to location data protection and the personality trait of conviviality. It can be seen that the more sociable and extrovert people are, the less they care about the protection of their location data. That is, people that enjoy being more often with other people are more relaxed with the idea of sharing their location, even with other parties. In Figure 2, we can see the relation between location data protection and whether the participants consider privacy to be time-dependent or not. It is apparent that particularly people who do not pay big attention to the protection of their location data, do not consider privacy to be time-dependent. The other way round, a large part of the people that care for their privacy and to whom location data protection is important, consider the sense of privacy to be changing over time. Our correlation analysis resulted in a two-tailed significance of 0.03 and a Pearson correlation coefficient of -0.302, which underpins the indication of an inverse correlation between the two items. Figure 3 presents the results of the belief that privacy is a time-dependent feature in relation to the participants' affinity for technology. What stands out in this figure is that solely

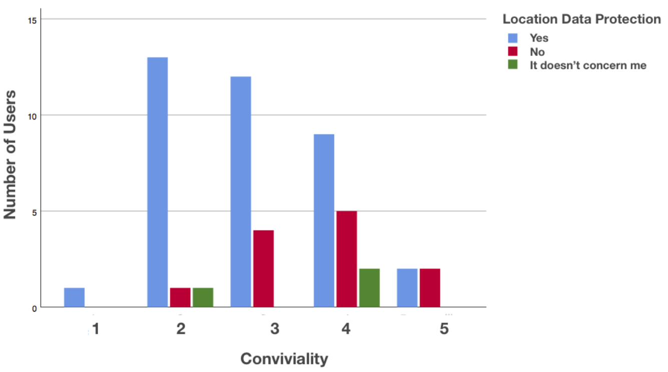


Fig. 1. Conviviality vs. Location data protection.
1: self-effacing and introvert, **5**: sociable and extrovert.
"**Yes**" represents: "Yes, Location data protection is important to me".

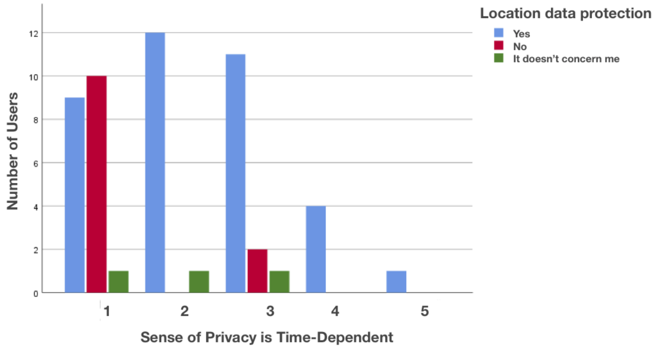


Fig. 2. Time-dependent sense of privacy vs. Location data protection.
1: "No, it isn't time-dependent", **5**: "Yes, it is time-dependent".
"**Yes**" represents: "Yes, Location data protection is important to me".

people with a strong affinity to technology take the view that privacy is indeed a time-dependent feature. This can be partly attributed to the fact that people interested in technology, know more about its potential, both positive and negative one. Thus, they might be more aware of situations where sharing location data can be critical and where flexible, time-dependent privacy rules could be of great importance. In general, it has been noticed that the interviewees have very divergent views on data protection and privacy. Some participants were not interested in data protection at all and have no problem being tracked everywhere and at any time. Other, however, consider data protection to be extremely important and want to be tracked as little as possible or even not at all. A significant group of the participant lie in-between by stating that they agree with sharing their location data only when it is necessary or brings practical benefits with it, e.g., for navigation purposes.

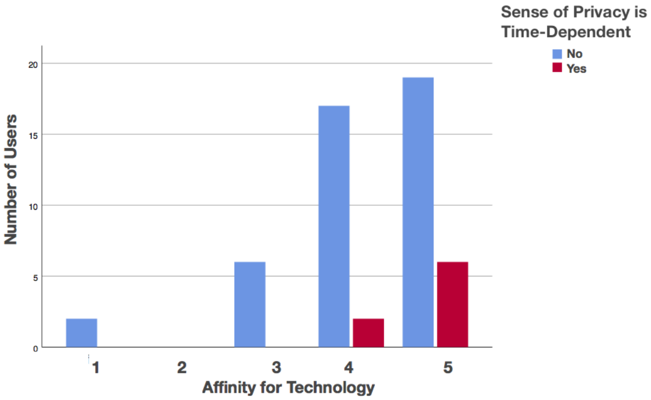


Fig. 3. Affinity for technology vs. Sense of privacy is time-dependent.
1: "I'm not interested in technology", **5**: "I'm very interested in technology".

IV. User Study II

A. Overview - Description

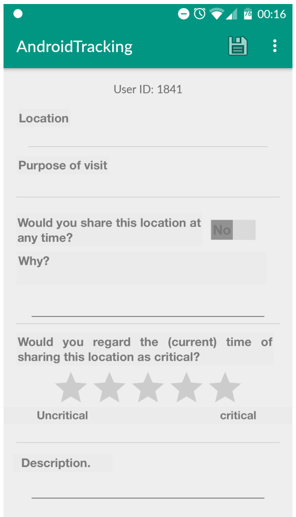
This section discusses our experimental study. Scope of this study was to identify existing time-dependencies with respect to privacy concerns in a real-world dataset scenario and confirm this way the results of our survey described in the previous Section III. During our experiment, we tracked a total of 10 mobile phone users over a period of 4 weeks. In addition to the GPS tracking running in the background, the users were asked to provide additional information or answer a small set of questions whenever they changed their location as described below:

- **Location type:** E.g., "restaurant", "chinese restaurant", etc.
- **Purpose of visit:** E.g., "Eating with friends/family", "celebrating Christmas party", etc.
- **Would you share this location at any time?** "Yes", "No". In case of "No", the user is additionally asked to add the reason.
- **Rating bar:** The user is asked to rate the experienced intrusion of his privacy with respect to sharing her current location, whereby
  1 star = "Uncritical, I have no problems with being tracked right now".
  5 stars = "Critical, I don't want people to know where I am right now".
- **Description:** E.g., "Critical, because no one should know that I am at a party," or "Not critical, because everyone knows that I am working here anyway".

For this purpose, we designed and implemented an Android tracking and annotation app illustrated in Figure 4. During the user study, both GPS and annotation data were encrypted and stored locally in the users' own devices in order to comply with the data protection guidelines. Each app user was assigned with a random User-ID. The per User-ID anonymized data were then transmitted to us after the study was over. Finally, we offered 3 Amazon coupons to the 3 participants that used our app at most, that is, with the most annotated entries, as an additional incentive for the participants of our study.

B. Evaluation

First, we preprocessed the data by filtering out inconsistencies and missing values. The filtered data were then organized in tables according to the type of information, e.g., "user-ID",



00:16

AndroidTracking

User ID: 1841

Location

Purpose of visit

Would you share this location at any time? No

Why?

Would you regard the (current) time of sharing this location as critical?

☆☆☆☆☆

Uncritical critical

Description.

Fig. 4. Screenshot of our Android tracking and annotation app.

"timestamp", "location label", "purpose", etc. We evaluated potential temporal dependencies in our data with regard to following aspects:

- Absolute time of day., e.g., 12:35pm, etc.
- Aggregated time of day in blocks:
  - 6am-10am: "morning"
  - 10am-12am: "mid-morning"
  - 12am-14pm: "midday"
  - 14pm-17pm: "afternoon"
  - 17pm-21pm: "evening"
  - 21pm-6am: "Night"
- Aggregated time in special blocks (events):
  - During the week
  - Weekend
  - Non-lecture period & Holidays
  - Christmas (24-26/12)
- Location category (based on the Foursquare venue taxonomy [26])
  - Residence
  - Work
  - Food
  - Business & Services
  - University
  - Culture & Entertainment
  - Nightlife
  - Natur & Leisure time
  - Travel & Traffic
  - Event
  - Others

The evaluation with respect to the location category is important in order to identify and exclude eventual impacts of the location type on the criticality rating of sharing the current location (from now on referred to as *privacy rating*).

We analyzed the data of each user both separately and combined. All in all, we had a total of 157 entries, which corresponds to an average of 5.61 entries per day. We calculated an average privacy rating of 1.847 and a standard deviation of 1.287, with 1 and 5 representing the least and the most critical score with regard to sharing the location at the corresponding moment, respectively. This is a relative low score. However, the data showed that 4 of our 10 users had no privacy concerns at all when it comes to sharing their location. They showed a permanent privacy rating of 1, regardless of time and place. This fact puled our average privacy rating down. Figure 5 presents the corresponding privacy rating distribution. The rating score 3 stands out as the second most frequently chosen rating. As being the middle rating value, it could be interpreted as users having occasionally substantial but not extreme concerns over their location privacy. The rest of the ratings are almost evenly spread out. Figure 6 contains the privacy ratings of all users distributed over the time of day. It can be seen that the privacy ratings are spread out over the range 1 to 5 without forming any identifiable patterns with respect to time. We can see the dense concentration of 1 values that reflects the ratings of the aforementioned "biased" users. We can also see the second dense concentration of 3 values. At first glance, despite the results of our first study, time appears to have no effect on the users' privacy concerns. However, after analyzing the data of single users separately, we could indeed find evidence of temporal dependencies. Figure 7 shows the privacy rating distribution over time for user ID4775. What is striking in this figure is that the particular user stated to be more sensitive when it comes to sharing her location in the afternoon hours between 14pm-20pm. A similar effect could be partly observed in other users as well. However, it should be noted here that high ratings came often in combination with certain location categories as well, such as outdoor and nightlife locations or friend's homes. Thus, it might be the location types that affect at most the users' sense of privacy. On the other hand, since certain locations are visited only during specific times, this could be again indirectly interpreted as a time-dependent effect as well, an effect that appears to be rather user-specific.

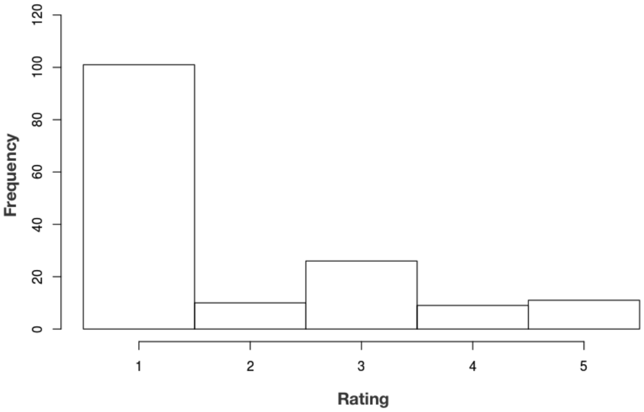


Fig. 5. Privacy ratings distribution over all users. 1 and 5 represent the least and the most critical private rating score respectively.

In Figure 8, we aggregate the time of day into 6 blocks.

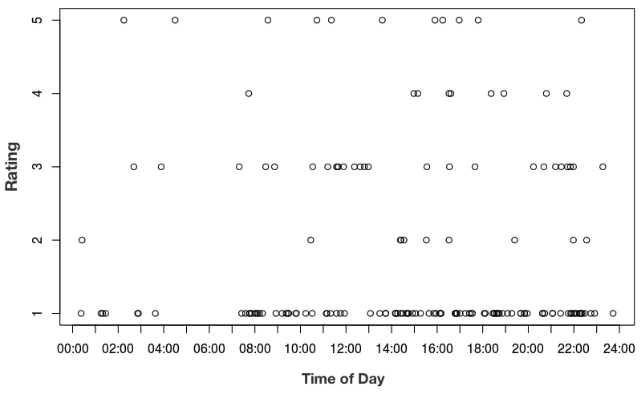


Fig. 6. Privacy ratings of all users over time of day. 1 and 5 represent the least and the most critical private rating score respectively.

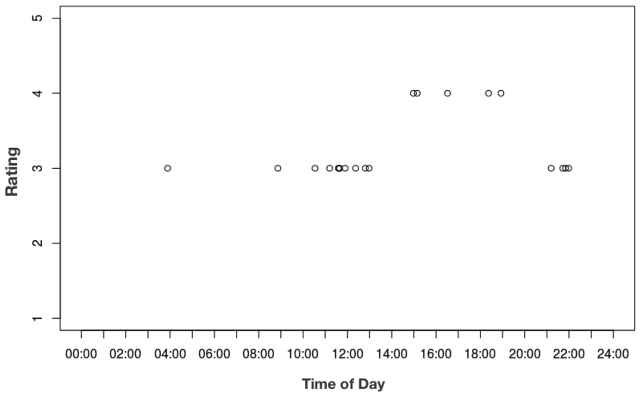


Fig. 7. Privacy ratings of user ID4775 over time of day. 1 and 5 represent the least and the most critical private rating score respectively.

Interestingly, both the mid-morning and the midday show an elevated average privacy rating of 2.24 and 2.33. However, at the same time, both show the least recorded entries, which may have affected to a certain degree the averages. Furthermore, no significant differences could be observed when we compared the ratings of during the week with the ones of the weekend. The Christmas period seemed to be having a slight effect on some users as we could observe a slight raise of high criticality rating values in the particular period (24-26 December). This could be attributed to the fact that people tend to concern more about their location privacy in their free time, when they are going out and when they are visiting relatives and close friends. Finally, an interesting result could be observed with regard to the location "home". Although "home" is a generally highly private location, the privacy ratings do change significantly over time, a fact that once again underpins our hypothesis that privacy concerns are time-dependent.

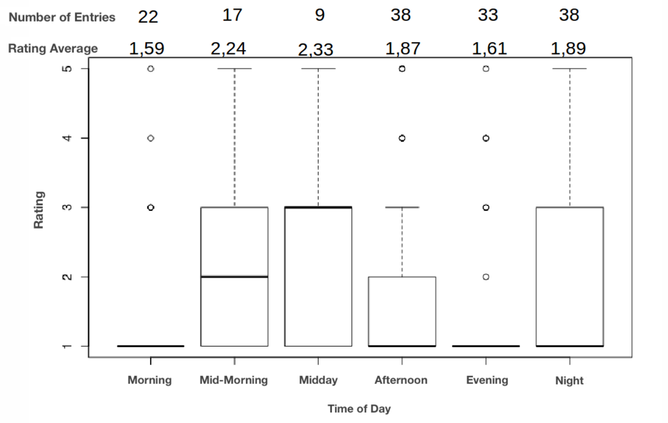


Fig. 8. Privacy ratings of all users over aggregated time blocks. 1 and 5 represent the least and the most critical private rating score respectively.

V. Conclusion

Recent research has been increasingly working on developing ways to protect the users' location data, with most focusing on spatial or semantic obfuscation techniques. However, very few seem to have investigated the impact of time on the users' privacy concerns. In the presented work, we attempt to explore time as a factor influencing the willingness of users to provide information about their location. In order to achieve this, we conducted 2 separate user studies, an online user survey as well as a 4-week long experimental study. Our analysis revealed slight, yet still present, evidence of an existing dependency between time and people's sense of privacy. The effect seems to be user-specific and is more common in people that are strong advocates of data protection. Certain personality traits, such as conviviality, also appear to play a significant role on the existence of time-dependencies. Overall, the presented results strengthen the need for dynamic, time-dependent location data protection techniques.

Acknowledgment

The authors would like to thank all of our user study participants, as well as Corbinian Grimm, Dennis Brüstle and Kevin Kellner for their contribution to the Android app design.

References

[1] eMarketer. (2015) Key trends in mobile advertising. [Online]. Available: https://www.statista.com/statistics/436071/location-based-service-users-usa/

[2] C. Parent *et al.*, "Semantic trajectories modeling and analysis," *ACM Computing Surveys (CSUR)*, vol. 45, no. 4, p. 42, 2013.

[3] A. Karatzoglou, H. Sentürk, A. Jablonski, and M. Beigl, "Applying artificial neural networks on two-layer semantic trajectories for predicting the next semantic location," in *International Conference on Artificial Neural Networks*. Springer, 2017, pp. 233–241.

[4] A. Karatzoglou, S. C. Lamp, and M. Beigl, "Matrix factorization on semantic trajectories for predicting future semantic locations," in *Wireless and Mobile Computing, Networking and Communications (WiMob),*. IEEE, 2017, pp. 1–7.

[5] J. J.-C. Ying, W.-C. Lee, T.-C. Weng, and V. S. Tseng, "Semantic trajectory mining for location prediction," in *Proceedings of the 19th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*. ACM, 2011, pp. 34–43.

[6] A. Karatzoglou, D. Köhler, and M. Beigl, "Purpose-of-visit-driven semantic similarity analysis on semantic trajectories for enhancing the future location prediction," in *2018 IEEE International Conference on Pervasive Computing and Communications (PerCom) Workshop Proceedings*. IEEE, 2018.

[7] J. L. Boyles, A. Smith, and M. Madden, "Privacy and data management on mobile devices," *Pew Research Center's Internet & American Life Project*, 2012.

[8] Zickuhr, “Location-based services,” *Pew Research Center’s Internet & American Life Project*, 2013.

[9] Y. Wang, “Privacy-enhancing technologies,” in *Handbook of research on social and organizational liabilities in information security*. IGI Global, 2009, pp. 203–227.

[10] M. Langheinrich, “Privacy by design?principles of privacy-aware ubiquitous systems,” in *International conference on Ubiquitous Computing*. Springer, 2001, pp. 273–291.

[11] D. E. Seidl, P. Jankowski, and M.-H. Tsou, “Privacy and spatial pattern preservation in masked gps trajectory data,” *International Journal of Geographical Information Science*, vol. 30, no. 4, pp. 785–800, 2016.

[12] L. Sweeney, “K-anonymity: A model for protecting privacy,” *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, pp. 557–570, 2002.

[13] S. T. Margulis, “On the status and contribution of westin’s and altman’s theories of privacy,” *Journal of Social Issues*, vol. 59, no. 2, pp. 411–429, 2003.

[14] A. F. Westin and O. M. Ruebhausen, *Privacy and freedom*. Atheneum New York, 1967, vol. 1.

[15] A. Westin, “Opinion surveys: What consumers have to say about information privacy,” *Prepared Witness Testimony, The House Committee on Energy and Commerce*, 2001.

[16] N. J. Marshall, “Dimensions of privacy preferences,” *Multivariate Behaviour Research*, vol. 9, no. 3, pp. 255–272, 1974.

[17] I. Altman, “Privacy regulation: Culturally universal or culturally specific?” *Journal of Social Issues*, vol. 33, no. 3, pp. 66–84, 1977.

[18] N. Zhang, C. Wang, and Y. Xu, “Privacy in online social networks,” 2011, CiteSeer.

[19] M. Moloney and F. Bannister, “A privacy control theory for online environments,” in *System Sciences, 2009. HICSS’09. 42nd Hawaii International Conference on*. IEEE, 2009, pp. 1–10.

[20] B. Lee, J. Oh, H. Yu, and J. Kim, “Protecting location privacy using location semantics,” in *Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ser. KDD ’11. ACM, 2011, pp. 1289–1297.

[21] T. Xu and Y. Cai, “Feeling-based location privacy protection for location-based services,” in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS ’09. ACM, 2009, pp. 348–357.

[22] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, “L-diversity: Privacy beyond k-anonymity,” *ACM Trans. Knowl. Discov. Data*, 2007.

[23] M. L. Damiani, C. Silvestri, and E. Bertino, “Fine-grained cloaking of sensitive positions in location-sharing applications,” *IEEE Pervasive Computing*, no. 4, pp. 64–72, 2011.

[24] L. Marconi, R. Di Pietro, B. Crispo, and M. Conti, “Time warp: How time affects privacy in lbss,” in *Information and Communications Security*, M. Soriano, S. Qing, and J. López, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 325–339.

[25] Google. (2018) Google forms. [Online]. Available: https://www.google.com/forms/

[26] Foursquare. (2018) Venue categories. [Online]. Available: https://developer.foursquare.com/docs/resources/categories