

Usable Privacy in Location-Based Services: The Need for a Regulatory Framework

Björn Beringer(✉), Per Ole Uphaus, and Harald Rau

Institute for Media Management, Ostfalia University of Applied Sciences, Salzgitter, Germany
{bjo.beringer,pe.uphaus,h.rau}@ostfalia.de

Abstract. Facing the last decades of information technology, the importance of 'usable privacy and security' (UPS) increased significantly. Previous studies have uncovered a tremendous gap in UPS-related research, especially concerning location-based services (LBS). This contribution aims to reduce this gap by identifying factors leading to a more user-centric design of LBS. It relies on guided interviews with international experts either with a scientific or an entrepreneurial background. The findings support solutions equipping the user with more control of owned data, thus ensuring more self-determination and decision-making authority affecting personal information. The study makes use of a qualitative content analysis in order to identify relevant factors that reveal which data security-related aspects are important by designing location-based services. The findings lead to two key outcomes: Firstly, the implementation of easier to use data security tools in applications based on LBS often comes with an information overload affecting the user. Secondly, a regulatory framework for third party vendors, users, and providers to address the lack of knowledge for user-friendly LBS turns out to be the key requirement for successful implementation of UPS.

Keywords: Location-based services · Usable privacy and security · Regulatory framework

1 Introduction

Dealing with aspects of data security in particular, users are increasingly faced with difficulties in understanding what is happening with their data and how to still maintain control [1, 2]. Research identified several problems regarding the use of mobile applications and the possibility of data control [3], involving the compatibility of data security, data protection and user-friendliness in applications using location-based services (LBS). In this regard, Abbas et al. favor a framework that accounts for the complexity of LBS applications in regulatory terms [1]. Given that, this contribution examines factors supporting usable data security while designing location-based services. By that, new insights into the relationship between location-based services (LBS) and Usable Privacy and Security will be generated, and factors influencing user-friendly data security in location-based technologies will be identified. Doing so, this study represents an important contribution in current research about regulatory considerations and ethical

© Springer Nature Switzerland AG 2021
O. Gervasi et al. (Eds.): ICCSA 2021, LNCS 12950, pp. 571–579, 2021.
https://doi.org/10.1007/978-3-030-86960-1_40

dilemmas [1]. For that purpose, interviews with international experts were conducted and analyzed. As an outcome, the opportunities and risks of UPS implementation in LBS will be summarized in several hypotheses for further research in the field. Above all, the results show a clear requirement for a framework covering socio-ethical, regulatory, and technological factors.

2 Theoretical Background

Mobile applications are increasingly becoming an essential part of people's everyday lives [4]. Depending on the user's context, LBS applications are able to deliver relevant, contextual information tailored to the current situation [5]. Data transmission of information tailored to the user's location often takes place via networks such as Wi-Fi as well as via mobile networks (GSM). Discussing the providers' part, servers receive the corresponding requests from the user and initiates the processing – depending on the service [6], to be exact: content and data servers respond to the user requests in a context-sensitive response way, and in some cases they also draw on the data of third-party providers [7]. During the use of LBS, data is generated, that is collected, stored, and processed on these servers of providers *and* third-party providers [8]. Data security is usually represented by means of a server with appropriate security functions and legally secured by data protection regulations [9]. Due to the access of the LBS provider or any third-party providers to the user's location and the collection of personal data, there are a number of security risks that may impact LBS usage [8]. Common security risks while using LBS that are frequently discussed in literature include the accessibility of personal information such as addresses, consumption characteristics, and places visited and corresponding times of stay for third parties without the user's permission [10, 11]. The increased risk of compromised privacy in LBS is considered to make the protection of privacy the greatest challenge within these technologies [12]. Despite their individual nature by focusing on sensitive security risks, LBS can be grouped, using the concept of 'location privacy' [13, 14].

Privacy is the *most frequently* considered issue when it comes to concerns during the use of mobile applications – especially location-based applications [15, 16]. This would include (but is not limited to) acts of extortion, tracking, surveillance, or intrusion [17, 18]. How exactly security risks are to be reduced and how new technologies can be created to be more user-friendly, and – at the same time – more secure, is summarized under the catchphrase of 'Usable Privacy and Security' (UPS). Saltzer and Schroeder were the first to mention a computer systems' easiness of use while also providing the highest possible level of security for the user [19]. Therefore, it seems to be important to integrate usability testing cycles into the design process of applications instead of testing and adapting them after development [20]. With these findings, they laid the foundation for today's 'Usable Privacy and Security' research. According to Naqvi and Porras, it is relevant to create a 'match' between system-internal development processes and the user's cognition [21]. The incorporation of the user's values into the design of safety systems enables the user's security-relevant needs and values to be met while harmonizing all security precautions [21]. Implementing this endeavor would presume a kind of education of the users and/or the incorporation of human aspects into the design

process for security systems [21]. A fundamental approach in UPS research today is to analyze the development of behavioral and activity-based safety systems – and one of the most relevant tasks then will be the reduction of safety tasks or prompts on users [22]. According to Atzeni et al., users always strive to pursue a goal or satisfy a need when using applications [23]. Therefore, systems should be designed in such a way that these goals can be achieved as quickly as possible, and in a secure way.

In summary: security aspects should be designed to be as user-friendly as possible; they must not hinder the user's search for information in order to avoid potential mistakes in the human interaction with the system [23]. Consequently, the target for researching this field is to identify ways to develop secure *and* 'usable' systems – systems, that do not restrict or frame users, while at the same time taking their individual needs into account [22, 24].

3 Methodology

In order to identify factors influencing possible correlations between user-friendly data security and LBS, guided interviews with experts were conducted and subsequently analyzed, making use of a qualitative content analysis. The sample consisted of 21 international and multidisciplinary participants from academia as well as from industry. All business representatives interviewed are coming with an entrepreneurial approach. An overview of the entire sample can be found in Table 1. To generate a sound set of qualitative data, all interviews were based on a guideline comprising the following overarching and for the coding process predefined dimensions, which provided the structure and ensured comparability of the individual interviews [25]: *meaning of location*, *security risks for location-based services*, *usability aspects*, *barriers of implementation*, and *future expectations* in this field. This contribution will focus explicitly on the barriers going along with security risks, as this dimension turned out to be particularly insightful. The identified barriers offer several invitations for further research and they provide deep insights how to implement UPS in location-based services. The interviews were recorded, transcribed, and coded using the QDA software MAXQDA. The interpretation made use of Mayring's qualitative content analysis – an approach considered particularly suitable for a systematic, rule- and theory-guided analysis of text-based interviews [26]. Except for the previously mentioned dimensions – adopted from literature, and implemented directly into the interview guideline – the derivation of all the further upcoming categories followed an inductive approach. The used routine determined the abstraction level as well as the process of coding, evaluation, and identification of context units. Finally, the derivation of categories from the transcript's semantic content resulted in a category system of various categories and subcategories. With the coding being handled by only one of the authors, Krippendorff's Alpha test was used to estimate the intracoder reliability with exemplary interviews at the beginning, in the middle and at the end of the coding process. The results indicate acceptable values for the interviews tested in the beginning ($\alpha = 0.7275$), in the middle ($\alpha = 0.8426$) and in the end ($\alpha = 0.6956$) of the entire encoding process, indicating reliable coding. Further while validity was ensured by revising the categories during and after the encoding process [26].

Table 1. Sample overview

Abbrevation	Position	Organization	Area of expertise	Country
P1	Ph.D	University	Privacy and Security	USA
P2	Dr.	Institute	Privacy and Security	Germany
P3	Ph.D	Institute	Movement data in GIS	Austria
P4	Prof. Dr.	University	Media law	Germany
P5	Prof. Dr.		Locative media	USA
P6	Prof. Dr.		Digital Technologies	Singapore
P7	Prof. Dr.		Geo-Information	Austria
P8	App Designer	Company	Critical application software	Germany
P9	Dr.	University	Privacy and Security	USA
P10	Prof. Dr.		Media sociology	USA
P11	Dr.		Socio-technical systems	Australia
P12	Prof. Dr.		Privacy and Security	USA
P13	Ph.D		Privacy and Data Protection	Germany
P14	Prof. Dr.		Social Implications of Technology	USA
P15	Prof. Dr.		Geo-Information Science	Belgium
P16	Prof. Dr.		Data protection	Germany
P17	CTO	Company	Data protection consulting	Germany
P18	CEO	Non-Profit-Organization	Data protection	Germany
P19	CEO	Company	Trustworthy Technologies	Australia
P20	CEO		Software development	Germany
P21	CEO		Geo Marketing and media planning	Germany

4 Results

The final analysis of the interviews resulted in a fairly complex category system. The evaluation of individual code relations subsequently provided in-depth insights into the interrelationship between several categories. Clear advantages of UPS incorporation in LBS were revealed: above all, the category *data combination* (e.g., visited locations, time

spent, usage of camera) is of interest, because strong ties between UPS and LBS's usage for *marketing*, *profiling*, and *tracking* became apparent. Connecting a two-sided view to the whole development process for applications seems to result in an added value for both areas, UPS as well as LBS. Some statements of the participants could be summarized to the conclusion that three overarching categories may form a kind of 'framework' for user-friendly data security in LBS applications. To name them: *socio-ethical*, *regulatory* and *technological* factors. *Socio-ethical* factors often show the connection between particularly sensitive data – such as one's personal address, timeslots at which a user leaves the house – and data security risks. This was especially mentioned in the category of *GPS use*. Furthermore, *regulatory* factors play a significant role in the case of LBS-based profiling. The same applies to the delivery of location-based advertising depending on the user's location-based identification. When it comes to technological factors, the user identification seems to be of particular importance – more precisely: the creation of movement profiles is to be seen as a risk. Further findings clearly reveal several obstacles by combining user-friendly data security with LBS usability aspects. During the analysis, barriers from the providers' as well as the users' perspective could be identified. On the providers' side, the development effort required turns out to be a decisive barrier. As P1 puts it: "On the other hand, it's a curse because if you talk to developers, they absolutely hate it" (P1). This is accompanied by operational costs that providers have to spend, as well as accompanying business interests of third-party providers based on business relationships. According to participants P2, P3 and P4, nearly all third parties involved are more interested in collecting user data than in giving users more options for data security. On the user's side, the participants primarily observe obstacles arising from the *antipattern* phenomenon in connection with location-based advertising (P2, P3). In this regard, antipattern refers to "software design shortcomings that can negatively affect software quality, in particular maintainability" [27] instead of supporting user-friendliness. Another obstacle not to be neglected is a lack in the know-how of users – especially in the case of location-based advertising. Additionally, barriers in the form of an information overload when users themselves become responsible for data management (e.g., in order to provide more control about personal data) were frequently mentioned (P1, P6, P7). P9 summarizes the participants' basic understanding of data management quite aptly, stating "more information, more transparency and something else that goes hand in hand with that, obviously, is control" (P9). Despite the obvious possibility of an increase in control, the analysis shows that security aspects may also turn out to be conflicting or complicating factors – especially in the case of location-based profiling. Collectively, the participants endorse the call for more regulation and guidance by designing the aforementioned framework. "I do think it comes back to creating a framework, [a] code that can help guide the way [in] which [the LBS-application] is developed" (P10). The following hypotheses summarize the outcome of the content analysis:

1. The successful integration of UPS factors into LBS seems to require a regulatory framework covering the entire value chain of LBS. This includes all stakeholders, at governmental, economic, and civil society levels.

2. Embedding UPS factors into LBS applications increases the ability to control data security regulations. As a result, more responsibility and expertise on behalf of the user is mandatory.
3. By involving the user in the configuration of user-friendly systems, the danger of information overload arises. In this scenario, users may favor previously known systems that they perceive to be easier to use.
4. User-friendly data security in LBS applications is primarily prevented by antipatterns. The resulting obstacles may primarily affect the field of location-based advertising.
5. More data security for the user in LBS applications contradicts the business interests of third-party providers, who are mainly interested in collecting as much data as possible.

5 Discussion

For user-friendly data security to be part of the LBS application, the participants of the interview consider a current focus on effort and cost. However, the now obvious business interests of third parties can be outlined as a surprising result. From the participants' point of view, third parties in general are less interested in user-friendly data security than in gaining the most comprehensive collection and storage of user data possible. For these companies "the database itself is of course the treasure […] with which they will likely want to earn money in the future" (P4) in order, for example, to create movement profiles with regard to advertising strategies or marketing activities. The collection and analysis of data could be regarded as the focus of LBS usage, this was also confirmed in a study by Fischer, who examined tracking of location data in different LBS application scenarios (mobility, tourism and event, out-of-home advertising, and consumer research) [28]. A regulatory framework could provide a possible solution for this issue, as this study's findings suggest an overarching need for some kind of regulation concerning the application of user-friendly security to location-based services. According to the participants, this framework should include socio-ethical, regulatory and technological factors reflecting the requirements of a value chain for the joint benefit of all stakeholders involved. First attempts of such an approach can be found in the research of Abbas et al. [1]. This way, the users' lack of knowledge could be compensated, and a clear guideline for service providers, third-party providers and users could be established. Another advantage of user-friendly data security, according to the participants, could be an increased use of LBS in general, going along with significantly more control over personal data and its use. Consequently, user-friendly data security is expected to increase the app retention in mobile applications that use LBS technologies [4]. In the case of commercial use, this could be directly linked to an increased customer loyalty.

6 Conclusion

The study investigated factors influencing user-friendly data security in location-based services. The findings indicate an overarching need for a framework regulating the compatibility of user-friendly security and location-based services (P10). This framework

should include socio-ethical, regulatory and technological factors aligned with the interests of all stakeholders involved. With regard to possible security risks, it was revealed that both profiling and tracking [29] can involve a considerable risk. In terms of security risks, associations with criminally motivated use of LBS became apparent, as also mentioned by Michael and Michael [30]. Several barriers were identified to interfere with user-friendly data security in LBS usage: A significant additional expense (costs for personnel and development) on the part of the providers prevents LBS and UPS from being combined. As pointed out by several business representatives, user-friendly data security seems to be not compatible with a commercially oriented collection of user data. It could also be shown that this commercially oriented actors apparently expect regulatory restrictions, and, with that, governments incentivizing user-friendly data security. Strategic communication and the concept of privacy by design [31], on the other hand were said to play a subordinate role and considered to be not significant. Potential factors having a positive influence on the data management also had been identified. An increased control over one's own data and the possibility of data minimization are two of them. From the scientists' point of view, it is precisely these two aspects that have a key function in harmonizing user-friendly data security and LBS. However, above all, currently, the user side appears to be characterized by antipatterns. At the same time, an increasing differentiation of usage can overwhelm the end user. Despite clear obstacles mentioned by all participants, there are outstanding advantages that exert a clearly positive effects on user-friendly data security and LBS: On the one hand, extensive legal regulations, such as the GDPR (general data protection regulation) [32], are taking effect to minimize security risks and obstacles – as also evidenced by the anchoring of the principles of privacy by design in the GDPR [31]. On the other hand, an increased app usage in general could be highlighted by the use of user-friendly data security in LBS. This impact can be considered a possible success factor for the progression towards a framework for the compatibility of user-friendly data security in location-based services.

7 Limitations and Future Research

Although this study was conducted with great diligence, it was also subject to some limitations. With regard to the chosen method, the effect of social desirability may have had an impact on interviews [33]. The authors deliberately chose to apply the approach of Mayring [26] in order to evaluate all interviews. In this context, however, aligning with alternative, more internationally recognized methods for qualitative content analyses might be advisable in order to comply with the overarching topic's international character in future studies.

Further research in this area should deal with the design of a framework for in-depth results. In this context, it would be useful to investigate how this framework could be implemented under the GDPR and what relationships exist between the stakeholders. The results could supplement the set of rules of the GDPR with regard to location-based applications [1]. The international focus of this work is essentially to be regarded as a benefit. In order to deepen this perspective, it could prove useful to investigate and compare possible correlations between user-friendly data security and LBS in different (national) jurisdictions. For example, a study in the context of the 'California Consumer

Privacy Act' [34], a law protecting consumer rights in California, often mentioned by the participants, would appear reasonable. Based on the results of this work, the consideration of user-friendly data security in commercially used mobile applications, especially in location-based services, offers extensive opportunities for further research. Not least because of the further development of location-based services [35], this field of research can be expected to become even more relevant in the future.

References

1. Abbas, R., Michael, K., Michael, M.G.: The regulatory considerations and ethical dilemmas of location-based services (LBS). Info Technol. People **27**(1), 2–20 (2014)
2. Michael, K., Michael, M. G.: Innovative Automatic Identification and Location-Based Services. IGI Global, Hershey, PA (2009)
3. Cao, Y., Takagi, S., Xiao, Y., Xiong, L., Yoshikawa, M.: PANDA: policy-aware location privacy for epidemic surveillance. Proc. VLDB Endowment **13**(12), 3001–3004 (2020)
4. Heinemann, G.: Die Neuausrichtung des App- und Smartphone-Shopping. Springer Gabler, Wiesbaden (2018)
5. Parviainen, P., Tihinen, M., Kääriäinen, J., Teppola, S.: Tackling the digitalization challenge: how to benefit from digitalization in practice. Int. J. Inf. Syst. Proj. Manag. **5**(1), 63–77 (2017)
6. Singhal, M., Shukla, A.: Implementation of location based services in android using GPS and Web services. Int. J. Comput. Sci. Issues **9**(2), 237–242 (2012)
7. Wendt, A., Brand, M., Schüppstuhl, T.: Semantically enriched spatial modelling of industrial indoor environments enabling location-based services. In: Schüppstuhl, T., Tracht, K., Franke, J. (eds.): Tagungsband des 3. Kongresses Montage Handhabung Industrieroboter, pp. 111–121. Springer, Heidelberg (2018)
8. Zhou, T.: Understanding location-based services users' privacy concern. Internet Res. **27**(3), 506–519 (2017)
9. Dao, D., Rizos, C., Wang, J.: Location-based services: technical and business issues. GPS Solutions **6**(3), 169–178 (2002)
10. Asuquo, P., et al.: Security and privacy in location-based services for vehicular and mobile communications: an overview, challenges, and countermeasures. IEEE Internet Things J. **5**(6), 4778–4802 (2018)
11. Chen, L., et al.: Robustness, security and privacy in location-based services for future IoT: a survey. IEEE Access **5**, 8956–8977 (2017)
12. Farouk, F., Alkady, Y., Rizk, R.: Efficient privacy-preserving scheme for location based services in VANET system. IEEE Access **8**, 60101–60116 (2020)
13. Tefera, M.K., Yang, X., Sun, Q.T.: A survey of system architectures, privacy preservation, and main research challenges on location-based services. KSII Trans. Internet Inf. Syst. **13**(6), 3199–3218 (2019)
14. Aditya, P., Bhattacharjee, B., Druschel, P., Erdélyi, V., Lentz, M.: Brave new world. ACM SIGMOBILE Mob. Comput. Commun. Rev. **18**(3), 49–54 (2015)
15. He, Y., Chen, J.: User location privacy protection mechanism for location-based services. Digital Commun. Netw. Accepted Manuscript (2020)
16. Parmar, D., Rao, U.P.: Dummy generation-based privacy preservation for location-based services. In: ICDCN 2020: Proceedings of the 21st International Conference on Distributed Computing and Networking, pp. 1. ACM, New York, NY (2020)
17. Abul, O., Bayrak, C.: From location to location pattern privacy in location-based services. Knowl. Inf. Syst. **56**(3), 533–557 (2018). https://doi.org/10.1007/s10115-017-1146-x

18. Sun, G., et al.: Location privacy preservation for mobile users in location-based services. IEEE Access **7**, 87425–87438 (2019)
19. Saltzer, J., Schroeder, M.: The protection of information in computer systems. In: Proceedings of the IEEE 1975, vol. 63, pp. 1278–1308 (1975)
20. Zurko, M.E., Simon, R.T.: User-centered security. In: Haigh, T., Hosmer, H (eds.) Proceedings of the 1996 workshop on New security paradigms – NSPW '1996, the 1996 workshop, pp. 27–33. ACM Press, New York, NY (1996)
21. Naqvi, B., Porras, J.: Usable security by design: a pattern approach. In: Moallem, A. (ed.) HCII 2020. LNCS, vol. 12210, pp. 609–618. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-50309-3_41
22. Cranor, L.F., Buchler, N.: Better together: usability and security go hand in hand. IEEE Secur. Priv. **12**(6), 89–93 (2014)
23. Atzeni, A., Faily, S., Galloni, R.: Usable security. In: Khosrow-Pour, M. (ed.): Advanced Methodologies and Technologies in System Security, Information Privacy, and Forensics, pp. 348–359 (2018)
24. Alt, F., von Zezschwitz, E.: Emerging trends in usable security and privacy. i-com **18**(3), 189–195 (2019)
25. Helfferich, C.: Leitfaden- und Experteninterviews. In: Baur, N., Blasius, J. (eds.) Handbuch Methoden der empirischen Sozialforschung, pp. 669–686. Springer VS, Wiesbaden (2019). https://doi.org/10.1007/978-3-658-21308-4_44
26. Mayring, P.: Qualitative content analysis. Forum Qual. Sozialforschung **1**(2), 20 (2000)
27. Fontana, F.A., Dietrich, J., Walter, B., Yamashita, A., Zanoni, M.: Antipattern and code smell false positives: preliminary conceptualization and classification. In: 2016 IEEE 23rd international conference on software analysis, evolution, and reengineering (SANER), pp. 609–613. IEEE, Piscataway, NJ (2016)
28. Fischer, B.: Mit einer Smartphone-App kontinuierlich Standortdaten erheben und Insights generieren. In: Keller, B., Klein, H.-W., Wachenfeld-Schell, A., Wirth, T. (eds.) Marktforschung für die Smart Data World, pp. 71–83. Springer, Wiesbaden (2020). https://doi.org/10.1007/978-3-658-28664-4_6
29. Bareth, U., Kupper, A.: Energy-efficient position tracking in proactive location-based services for smartphone environments. In: 2011 IEEE 35th Annual Computer Software and Applications Conference, pp. 516–521. IEEE, Piscataway, NJ (2011)
30. Michael, K., Michael, M.G.: The social and behavioural implications of location-based services. J. Location Based Serv. **5**(3–4), 121–137 (2011)
31. Cavoukian, A.: Understanding how to implement privacy by design, one step at a time. IEEE Consum. Electr. Mag. **9**(2), 78–82 (2020)
32. Schiering, I., Mester, B.A., Friedewald, M., Martin, N., Hallinan, D.: Datenschutz-Risiken partizipativ identifizieren und analysieren. Datenschutz und Datensicherheit **44**(3), 161–165 (2020)
33. Reuband, K.-H.: Soziale Erwünschtheit und unzureichende Erinnerung als Fehlerquelle im Interview: Möglichkeiten und Grenzen bei der Rekonstruktion von früherem Verhalten – das Beispiel Drogengebrauch. Zentralarchiv für Empirische Sozialforschung **23**, 63–72 (1988)
34. Aridor, G., Che, Y.-K., Nelson, W., Salz, T.: The economic consequences of data privacy regulation: empirical evidence from GDPR. In: SSRN Electronic Journal (2020)
35. Göll, N., Lassnig, M., Rehrl, K.: Location Based Services im Tourismus – Quo Vadis? In: Egger, R., Jooss, M. (eds.): mTourism – Mobile Dienste im Tourismus, pp. 27–44. Gabler, Wiesbaden (2010)