Location Data Privacy : Principles to Practice

Mehrnaz Ataei

Westfälische Wilhelms-Universität Münster

Doctoral Dissertation

Location Data Privacy : Principles to Practice

Inaugural dissertation in fulfillment of the academic degree of

Doctor of Natural Sciences (Dr. rer. nat.)

in the Department of Geosciences
of the Faculty of Mathematics and Natural Sciences
of the Westfälische Wilhelms-Universität Münster

Submitted by
Mehrnaz Ataei
from Tehran, Iran
- 2018 -

Dean: Prof. Dr. Harald Strausß
First supervisor: Prof. Dr.-Ing Christian Kray(First reviewer)
Second supervisor: Dr. Vitor Santos(Second reviewer)
Third supervisor: Dr. Francisco Ramos
Cover design: Anders Lindström

Day of defence: _____
Day of promotion: _____

48149 Münster, Germany

European Joint Doctorate in Geoinformatics: Enabling Open Cities
Marie Skłodowska-Curie Action (ITN-EJD)

Abstract

Location data is essential to the provision of relevant and tailored information in location-based services (LBS) but has the potential to reveal sensitive information about users. Unwanted disclosure of location data is associated with various threats known as *dataveillance* which can lead to risks like loss of control, (continuous) monitoring, identification, and social profiling. Striking a balance between providing a service based on the user's location while protecting their (location) privacy is thus a key challenge in this area. Although many solutions have been developed to mitigate the data privacy-related threats, the aspects involving users (i.e. User Interfaces (UI)) and the way in which location data management can affects (location) data privacy have not received much attention in the literature.

This thesis develops and evaluates approaches to facilitate the design and development of privacy-aware LBS. This work has explicitly focused on three areas: location data management in LBS, the design of UI for LBS, and compliance with (location) data privacy regulation. To address location data management, this thesis proposes modifications to LBS architectures and introduces the concept of temporal and spatial ephemerality as an alternative way to manage location privacy. The modifications include adding two components to the LBS architecture: one component dedicated to the management of decisions regarding collected location data such as applying restriction on the time that the service provider stores the data; and one component for adjusting location data privacy settings for the users of LBS. This thesis then develops a set of UI controls for fine-grained management of location privacy settings based on privacy theory (Westin), privacy by design principles and general UI design principles. Finally, this thesis brings forth a set of guidelines for the design and development of privacy-aware LBS through the analysis of the General Data Protection Regulation (GDPR) and expert recommendations.

Service providers, designers, and developers of LBS can benefit from the contributions of this work as the proposed architecture and UI model can help them to recognise and address privacy issues during the LBS development process. The developed guidelines, on the other hand, can be helpful when developers and designers face difficulties understanding (location) data privacy-related regulations. The guidelines include both a list of legal requirements derived from GDPR's text and expert suggestions for developers and designers of LBS in the process of complying with data privacy regulation.

> *The pleasure we derive from journeys is perhaps dependent more on the mindset with which we travel than on the destination we travel to.*
>
> **— Alain de Botton**
> (The Art of Travel)

Acknowledgements

Now that I am at the destination and the thesis is ready, it is time to thank many people who made this possible. Christian Kray, you have been my supervisor, mentor, and support throughout the whole PhD journey. I am grateful for all those discussions that turned my blurry thoughts to sharp arguments. You were always there with your valuable advice, good company and lots of great ideas. I can not thank you enough!

Auriol Degbelo, I could not have done this without you. I have learned a lot from you, thank you for helping me to get through the difficult times, thank you for always being there, especially during those late and last minute paper submissions! You will always be an amazing source of inspiration! I would like to thank Vitor Santos, my second supervisor for the interesting discussions we had during my stay at Nova IMS. You inspired me to look at my research from a different perspective!

One often hears that doing PhD means lots of lonely moments. I was lucky to never experience that. I find myself fortunate to have worked at IFGI and the SITCOM lab - a fantastic environment, full of hard-working, intelligent, and caring people. Besides, I was lucky to be accompanied by a great team of GEO-C colleagues, you have made this journey enjoyable. Thank you all!

My special admiration goes to my office mates. I did not feel alone, because I was so lucky to have your friendships. Anita, thank you for being you! Samuel, thank you for being there for me, and Diego, thank you for choosing office 240. My morning coffees will taste different from now on!

Throughout my life, no matter what I have chosen, my parents have always been there to support me, Thank you Mahnaz! Thank you, Nabi! I'm so grateful to have parents like you! Special thanks to Lena, Bosse and Maria, you were amazingly supportive, and I'm thankful to have you in my life!

Behrad! Thank you for being there for me no matter what, your love and support, your presence and friendship are irreplaceable!

And last but not least, Anders, you have been there for me in every moment of this journey. I cherish our moments together, and words can not express my gratitude, I would not even be here without you! "go get it"! - You said!

This dissertation is funded by the European Commission within the Marie Skłodowska-Curie Actions (ITN-EJD). Grant Agreement num. 642332 - GEO-C - H2020-MSCA-ITN-2014.

Contents

List of Figures

List of Tables

1 Introduction

> *Arguing that you don't care about the right to privacy because you have nothing to hide, is no different than saying you don't care about free speech because you have nothing to say.*
>
> **— Edward Snowden**

1.1 Motivation

Location-based services (LBS) are technologies that provide information for users according to their geographical location (Junglas and Watson, 2008). Mobile services and positioning techniques support a variety of technologies with location-aware abilities in various areas such as navigation, social networking, marketing, safety, and entertainment. The defining feature of location-based services (LBS) is that they respond to the requests of users according to their physical location, which is not the case for other types of services (Schmitz Weiss, 2013). This dependency on positional information enables user-friendly services with abilities to deliver relevant information to users about their surroundings but also entails issues regarding location privacy. In principle, the location privacy of users can be compromised in two ways: (1) using real-time location information or (2) using past data. Unwanted disclosures of location data can lead to the use of personal data which enables "*dataveillance*", which is a systematic use of personal data for continuous monitoring of individual's communications and actions (Clarke 1988). Such monitoring and the disclosure of sensitive personal information about users can harm individuals in different ways, for instance, it can cause loss of control over one's private life, social sorting, and profiling (Abbas et al., 2015). Analysing past location data can also predict users' behaviour at any time in the future (Krumm, 2009). Therefore, there is a need for developing privacy-aware LBS which can create a balance between providing a service to users while protecting their location privacy.

1.2 Problem statement

Individuals are surrounded by various technologies that are constantly collecting their personal data. The ubiquitous nature of these technologies makes it difficult for the users to fully grasp the implications of their actions regarding the loss of their (location) data privacy. In order to receive the full benefits of a location-based service, users have to share location data, e.g., where they are, where they have been or where they are going to be. With systems continuously tracking users, or users actively reporting on their locations (e.g. through online check-ins), a large amount of potentially sensitive information is generated constantly (Beresford and Stajano, 2003). Such practices make it challenging for users to know what information these services are collecting, the reason it is being collected for, and who will have access to it (Schaub, Könings, et al., 2015). If location data collected by LBS is disclosed, this data could pose a serious threat to users' privacy and safety. A number of threats are associated with the leaked location information (Krumm, 2009). For instance, analysis of movement patterns enables the extraction of a broad range of sensitive user-related information. This includes the identity of the user, their (home) address, individual (points of) interests as well as events (e.g., such as strikes or protests) that a user participated in (Hoh et al., 2006; Patterson et al., 2003). Dataveillance, which is the systematic use of personal data to investigate or monitor the actions of people (Clarke, 1988) is also associated with the unwanted disclosure of personal (location) data. Abbas et al. (2015) states that dataveillance can lead to severe negative social implications for users, for example, the feeling of losing control over one's private life. The continuous monitoring and being constantly watched could have an impact on users social abilities such as being creative, different or diverse (K. Michael and M. Michael, 2011). "*It is not only the loss of privacy that is increasingly at risk but also the wonder of improvisation. We will be playing to a packed theatre instead of being comfortable in our own skins and identities*"(K. Michael and M. Michael, 2011).

Considerable (location) data privacy-related issues regarding the development of LBS become apparent when observing the risks and threats associated with the collection and use of location data. LBS providers have significant responsibilities in this regard. They have the power of contributing to the (location) data protection of LBS users through various means. Protecting location data will not only benefit users but eventually services providers as well. Accordingly, despite the focus of research on the technological development of LBS, limited work has been done to study the defining factors that influence LBS adoption by users, studies like Felt et al. (2012) have shown that users have concerns regarding privacy and that these concerns have an impact on the adoption of LBS (Zhou, 2011; Fodor and Brem, 2015). So by considering protection of users location privacy by service providers, transparency and trust will increase, and eventually, this might lead to broader adoption of LBS by users and consequently a more significant number of customers.

Various methods have been developed to mitigate threats associated with LBS. To point out the strengths and weakness of each method, this work has categorised them into three areas; Technical, UI-related (i.e. options to control location privacy and education for users), and legal-based methods.

Technical methods include privacy-enhancing Technologies (PET) such as anonymisation, obfuscation, or computational measures like spatial cloaking (Duckham and Kulik, 2006). PET deal with location privacy issues on a technical level, emphasising on how the location data should be collected, processed, used, and stored. PET then implement privacy-preserving methods in different stages of the processing. Despite its importance and use-fullness, PET suffer from limitations such as the risk of negative impact on the performance of the system or increased complexity. Another issue with PET is that they are mainly developed based on the assumption that (location) data is perpetually stored. The role of location data management with the assumption of keeping the (location) data as long as its needed for the functionality of the service and its impact on location data privacy has received little attention in previously conducted research. Thus, there is a need to develop methods for managing (location) data in order to protect location privacy.

UI-related methods are those that communicate the status of location data (e.g. collection, share, storage) through the UI of the service with its users and also provide privacy adjustment options for them. Such methods have been suggested in previous literature and a few services like Google privacy dashboard[1]. However, the issue in this context is related to the limited number of such examples and the little attention that have been paid to the increased complexity that such services can cause for user's interaction. In addition to UI elements, there is also a need to convey to the users the importance of protecting location data and also to teach them practical ways for protecting it. Such educational support is something that many current services do not have available for their users. Another problem is about the current practices of the existing applications and services, the majority of the apps request location data from users to provide a location-based service. Simultaneously, these apps offer only crude controls for location privacy settings (sharing all or nothing). The main problem is that there is a lack of options for users to control their location privacy while using a location-based service (e.g. whether they accept the "term & conditions" or not). Thus, there is a need to explore the possibility of providing appropriate controls and options for adjusting (location) data privacy for users of LBS).

Besides technical and UI-related methods, the third group of counter-measures are regulatory strategies. Understanding the legal requirements of data privacy legislation can turn into a challenge for LBS developers who eventually have to implement a service that complies with it. The General Data Protection Regulation (GDPR) is an example that harmonises data privacy laws across Europe but does

[1] https://myaccount.google.com/intro/dashboard

not provide clear guidelines for designers and developers to build services that comply with the law. Therefore there is a need to address the gap between legal data privacy regulation's requirements and understandable instructions for developers and designers.

To summarise, there are three areas in need of more profound understanding and insights that this work has highlighted; 1) Exploring location information management with a non-permanent storage approach and its impact on (location) data privacy. 2) Examining possible options to support the users of LBS regarding the adjustment of their location privacy. 3) Exploring the development of tools to help LBS developers to comply with privacy legislation while developing LBS. These three aspects are inherently connected and therefore need to be addressed at the same time. For instance, one can not respect the data subject's rights (i.e. an identifiable natural person (EU, 2016)) without designing UI elements for them to adjust their location data sharing.

1.3 Objectives

This section will present the main research question that is going to be investigated in this work. The goal of this thesis is to find out how location data privacy should be considered, managed, and integrated into the design and development process of LBS. Generating strategies to address privacy-related concerns in all stages of LBS development (design, implementation, and its final use) can improve the adoption process of LBS for current and future users (Wang and R.-L. Lin, 2017). Thus, the protection of location data could be considered as one of the key components for building a successful location-based service. Therefore, this work focuses on addressing location data privacy issues in the process of LBS development. The research questions revolve around three main objectives: 1) to explore the role of location information management on location privacy protection; 2) to find appropriate means to communicate location privacy through the UI of LBS and provide tools to users that allow them to control their location privacy; and 3) to develop tools to help developers to understand and implement privacy legislation requirements while developing LBS. Accordingly, the research question which is elaborated by three sub-questions is formulated and explained as follows:

Research Question: How should **location data privacy** be **considered**, **managed**, and **integrated** while developing a **location-based service**?

The overall objective of the thesis is to find out how to consider location privacy, realise how to manage it and eventually find out how to implement privacy-preserving measures in the process of LBS development. Before presenting the three guiding questions, it is essential to explain what this work refers to as "consideration", "management" and "integration" of location data privacy:

- **Consideration** refers to thinking thoroughly about location privacy and also discussing it before, during, and after developing a location-based service.

- **Management** refers to discussing every action related to location data including collection (e.g. what is going to be collected and why), processing (e.g. which part of the collected data is going to be processed and for what purposes), storage (i.e. where the data is going to be stored and for how long it is going to be kept), sharing (e.g. with whom the data is going to be shared and why), presentation (e.g. what part of the collected location data is going to be presented to the users or other parties and why), and communication (e.g. which parts of the location data management process is going to be communicated with users). Management is relevant to the consideration, as one has to initiate the discussion about privacy to make decisions about it but management's eventual goal is to implement practical privacy-preserving measure to improve the location privacy of end users.

- **Integration** refers to specifically designing and developing privacy-preserving measures and also including them in the body of the LBS (e.g. incorporating measures into the architecture or the UI) as well as the development process. Thus, integration includes practical and tangible changes which lead to the implementation of practical privacy-preserving measures for improving location privacy in LBS.

These three factors are inseparably connected to each other in the context of location data privacy research. One must consider location privacy in order to be able to eventually manage or integrate it for the improvement of the location protection during the process of LBS development. Therefore, the consideration factors is a repeating theme in addressing the guiding questions, the other two factors are also involved in all the guiding questions, but they might receive a different level of attention depending on the focus of the question. The three guiding questions of the work are as follows:

GQ1. How should location information be managed in LBS to protect location privacy? GQ1 examines the architecture of the LBS to find out first how different components are collecting, processing and storing location data, and also what could be changed in the architecture to improve the protection of location privacy.

GQ2. How should user interfaces of LBS be designed to provide users with means to make informed choices about their location privacy? GQ2 is about understanding how one can first understand and address location privacy at the UI level and then design UI elements specifically for adjusting location privacy settings of a location-based service.

GQ3. How to comply with privacy legislation while developing LBS? GQ3 addresses the gap between established (location) data privacy regulations' requirements and developers understandings of such requirements.

1.4 Scope

The various aspects involved in the subject of (location) data privacy create a complex and challenging area for those who want to address it. Nevertheless, it is possible to decrease the complexity of addressing (location) data privacy by breaking down the matter into manageable pieces and also select the specific context to address the issues regarding (location) data privacy. Previous research has discussed data privacy from different aspects such as psychological Brandeis and Warren (1890), technical, legal and, educational (Keßler and McKenzie, 2018). Prior works have tried to bridge those aspects, for instance using privacy definition from the field of psychology to define data privacy (D. J. Solove, 2005). While some like Keßler and McKenzie (2018) argue that the data privacy issues must be tackled as a whole, others like D. Solove (2008) argue that the issue should be broken down into smaller pieces and be discussed from various perspectives. This thesis is in favour of the latter approach; it has focused solely on the concept of location privacy in the context of data privacy and also selected the development process of LBS to emphasis on. The solutions developed were aimed at developers, designers, and also end users of LBS. It was also necessary for this work to limit the legal aspects of its studies. Therefore, as this research is conducted in Germany and Portugal, only the European Union (EU) legislation for data privacy was considered in the current research. To summarise, the aim of the study was limited to addressing the consideration, management and integration of location data privacy in the development process of LBS, based on General Data Privacy Regulation of EU.

1.5 Methodology

A number of methods were applied to answer the research question and associated guiding questions. The majority of the methods used were selected from the field of Human-Computer Interaction (HCI) (Lazar et al., 2017) and the rest were standard user research methods for data collection and analysis. This work had to adjust some of the methods in order to make them appropriate for the conducted studies. The adjustments done will be explained in detail when describing the studies in each respective chapter. Table 1.1 lists the methods and their usage for answering each of the questions. The last column of the table also shows the chapters where the method were used.

The research process started with formulating the research question through an initial literature review. The second round of the literature review aimed at performing a critical evaluation of previous research, conducted in the field of LBS development with respect to location data privacy (the result is presented in chapter 2). The literature review method was used to address all three guiding questions. The research process continued by applying structured and semi-structured interviews and, surveys to collect qualitative data. Interviews are a well-known method in the field of HCI to collect in-depth data. Lazar et al. (2017) argue that while results collected from surveys is general, interviews results are deep, "*direct conversation with fewer participants can provide perspectives and useful data that surveys might miss*" (Lazar et al., 2017). Therefore, this work selected surveys and interviews together to cover various aspects at different levels. Regarding the type of the interviews conducted in this work, the method of using structured interview was selected during the evaluation of the proposed UI elements (i.e. chapter 3), which took place in a setting where it was essential that all the users received the same questions and information. For discussing the implementation of the GDPR with experts in chapter 4, a semi-structured interview method was selected. This method was selected because in that context it was important to be flexible and gather information from different perspectives. Prototyping (Budde et al., 1992) was also a method applied in chapter 3 and 4 for evaluating the proposed concepts and solutions (see Table 1.1). Prototyping is a quick and powerful tool for gathering data about user's experiences in early stages of service or product development. The studies conducted in this thesis used high-fidelity prototypes which users could use on mobile phones, the prototyping method was helpful to gather insights about users' perceptions and preferences regarding the proposed ideas. Finally, both qualitative and quantitative data analysis methods were applied to analyse the collected data through user studies (including interviews, surveys, and user evaluations). MAXQAD and Stata are the two softwares that were used to run the qualitative and quantitative data analysis presented in this work.

Method	GQ1	GQ2	GQ3	Chapter
Literature review	✓	✓	✓	C2.C3.C4
Structured interview		✓		C3.C4
Semi-structured Interview		✓	✓	C3.C4
Survey			✓	C4
Prototyping	✓	✓	✓	C3.C4

Tab. 1.1: List of the methods, the corresponding guiding questions and chapters that used them in this thesis.

1.6 Overview

While each of the next three chapters of this thesis is going to address one of the guiding questions, the presented solutions are not restricted to only one aspect of the main research question. Figure 1.1 shows the outline of the thesis. It presents the connections between chapters and the the guiding questions as well as the summary of the approaches that have been used to address main research question.

The structure of the following chapters follows the process of addressing the guiding questions which ultimately resulted in answering the main research question. Chapter 2 provides a background on (location) data privacy and LBS. It then introduces the concept of ephemerality and also proposes a modification to the architecture of LBS following privacy by design principles with the aim of improving (location) data privacy protection. Ideas developed in chapter 3 were initially based on one of the changes proposed in Chapter 2. Chapter 3 also provides a detailed background on various aspects of location privacy in the context of UI design. It presents a theoretical model and a set of UI design elements for adjusting location privacy settings in LBS. Chapter 4 presents an approach for bridging the gap between legal documents and practical instructions for developers and designers of LBS. It also presents a process of developing a guideline as a practical example to address this gap. Discussion chapter (i.e. 5) takes a step back and discusses data privacy in general at the beginning and then highlights the benefits and the drawbacks of the findings. Finally, chapter 6 summarises the contributions and presents the conclusion. Table 1.2 presents the list of the manuscripts that constitute the different chapters of this work.

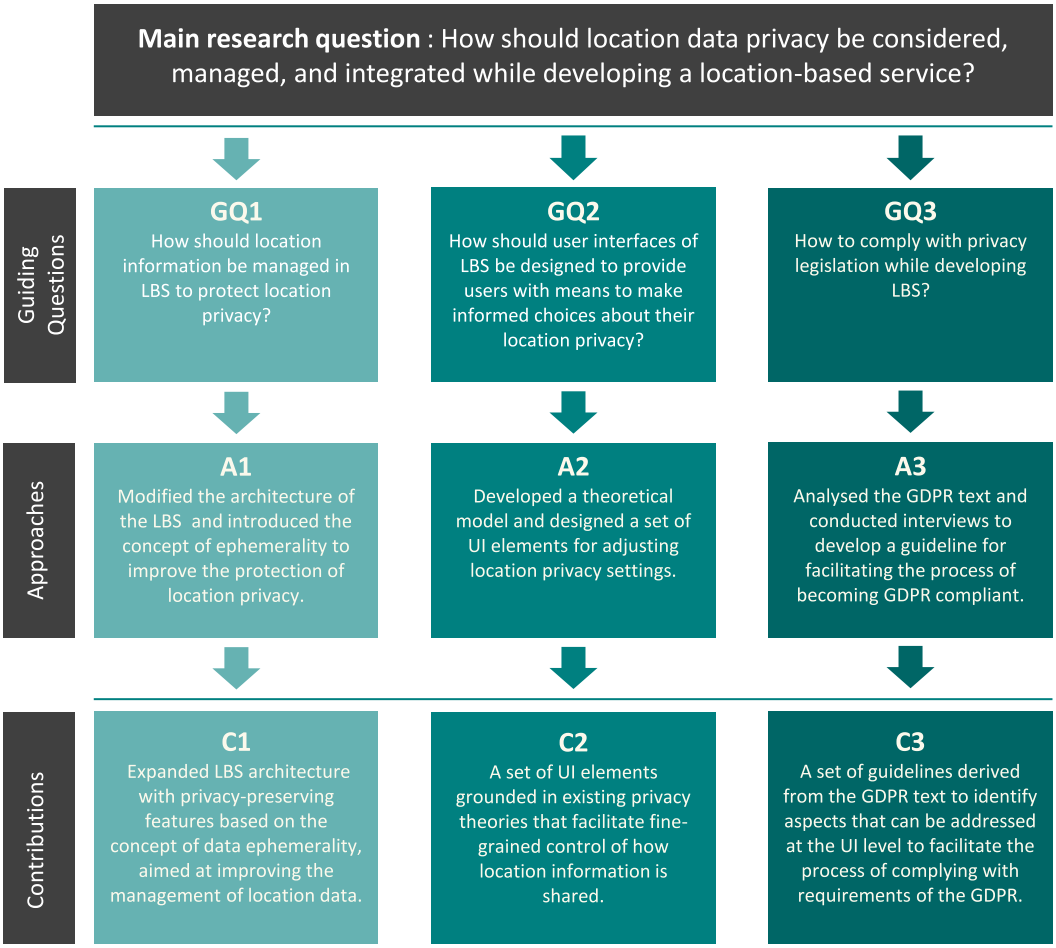


Fig. 1.1: Overview of the main and guiding research questions, approaches, and contributions.

Chapter	Manuscript	Guiding Question	Status
Chapter 2	Ataei M., Kray C. (2017) "Ephemerality Is the New Black: A Novel Perspective on Location Data Management and Location Privacy in LBS." In: Gartner G., Huang H. (eds) Progress in Location-Based Services 2016. Lecture Notes in Geoinformation and Cartography. Springer, Cham. https://doi.org/10.1007/978-3-319-47289-8_18.	GQ 1.	Published
Chapter 3	Ataei M., Degbelo A., Kray C. (2018) "Privacy theory in practice: Designing a user interface for managing location privacy on mobile devices." Journal of Location Based Services. https://doi.org/10.1080/17489725.2018.1511839.	GQ 2.	Accepted
Chapter 4	Ataei M., Degbelo A., Kray C., Santos V. (2018) "Complying with Privacy Legislation: From legal Text to Implementation of Privacy-Aware Location Based Services.	GQ 1. & GQ3	Submitted

Tab. 1.2: Manuscripts which constitute the chapters of this thesis.

2

Ephemerality Is the New Black: A Novel Perspective on Location Data Management and Location Privacy in LBS

> *There are no rules of architecture for a castle in the clouds.*
>
> — **Gilbert K. Chesterton**
> (The Everlasting Man)

This chapter was published in preparation for the 13th Conference on Location-Based Services as Ataei M., Kray C. (2017) "Ephemerality Is the New Black: A Novel Perspective on Location Data Management and Location Privacy in LBS." In: Gartner G., Huang H. (eds) Progress in Location-Based Services 2016. Lecture Notes in Geoinformation and Cartography. Springer, Cham. https://doi.org/10.1007/978-3-319-47289-8_18.

Location information is essential to location-based services (LBS), but also has the potential to reveal sensitive information about the users of LBS to malicious agents. Therefore, location privacy is an important issue to address for both users and providers of LBS. In this paper, we investigate how location privacy can be realized in the context of a location-based service. Based on a review of architectures for LBS and key issues related to location privacy, we discuss several measures to integrate location privacy into LBS. In order to address privacy threats associated with the storage of location information, we propose an approach based on privacy-by-design principles and introduce a conceptual model to facilitate the implementation of those principles. In addition, we investigate the role of location data management in the context of privacy preservation, and propose the concept of temporal and spatial ephemerality to improve location privacy in the context of a location-based service.

2.1 Introduction

The defining feature of location-based services (LBS) is that they respond to the requests of users according to their physical location, which is not the case for other types of services. This dependency on positional information enables new and more user-friendly services but also entails issues regarding location privacy (Junglas and Watson, 2008); (Barkhuus and Dey, 2003); (Fodor and Brem, 2015). Striking a balance between providing a service based on the user's location while protecting their (location) privacy is thus a key challenge in this area. In principle, the location privacy of users can be compromised in two ways: (1) using real-time location information enables an attacker to find you right now and carry out different attacks; (2) using past data facilitates the discovery of who you are, where you live, and what you do. It can be used, for example, to predict your behavior at any time in the future (Krumm, 2009). Ideally, issues related to location privacy are considered at design time, i.e. when a location-based service is developed. The 'Privacy by Design' approach (PbD) has been applied in other domains to "prevent privacy invasive events before they happen" (Cavoukian, 2010). It thus constitutes a good starting point for developing a process for building LBS that actively considers location privacy during the design process rather than tinkering with the service after location privacy has been compromised.

The work presented in this paper proposes a new model to realize location privacy by design and an approach to tackle location privacy by focusing on the management of location information in LBS. We also introduce the concept of ephemerality of location data and demonstrate how it can help to address privacy threats resulting from the retention of location data. The remainder of the paper is structured as follows. We first discuss different models and architectures that have been proposed to describe the structure and inner processes of LBS. Section three reviews different approaches to location privacy. The main part of the paper (section four) outlines the basic model underpinning our approach and then reviews in detail each element and strategy for location privacy protection. The penultimate section discusses the limitations and implications of our approach. The final section summarizes our key findings and provides an outlook on future research.

2.2 The Anatomy of LBS

Location-based services (LBS) cover a broad range of application scenarios, from navigation support (Ran et al., 2004) over local recommender systems (Foursquare, 2016a) to intelligent transport services (Foursquare, 2016b) and games (O'Hara, 2008). Such services are different from more conventional services as they are aware of the context in which they are being used and can adapt their contents

and presentation accordingly (Steiniger et al., 2008). While a traditional service usually only relies on networking and computing resources to "collect, process, filter, transmit, and disseminate data that represents information useful for a specific purpose or individual" (Schiller, 2004), a location-based service also intrinsically considers positional information. This enables a location-based service to deliver "information to its users in a highly selective manner, by taking the user's past, present, or future location and other context information into account" (Schiller, 2004). Consequently, a location-based service is subject to additional requirements compared to standard services (Chow and Mohamed F Mokbel, 2009) and its architecture may also differ to accommodate those requirements. In the following, we therefore review several architectures and models that have been proposed for LBS and analyze some examples of LBS with respect to how they function.

Kido et al. (2005) proposed a location-based service model that consists of a geographic information system (GIS), a service provider and a database. In their model, a user of a location-based service obtains their location through a positioning device and then sends the position data to a service provider. The service provider, in turn, creates a response after communicating with the database and the GIS. Spiekermann (2004) developed a general communication model, which includes three layers: the positioning layer, the application layer, and the middleware layer. The positioning layer calculates the position of a user. The application layer comprises all services that request location data to integrate it into their offering. The middleware layer sits between the positioning layer and the application layer in order to reduce the complexity of service integration. All layers access the GIS directly. Strassman and Collier (2004) also discuss the development of a location-based service, a commercial friend finder application (Schiller, 2004). The application is built around a location engine, which encapsulates the 'intelligence' of the service. It includes functionality such as geocoding, reverse geocoding, and routing, and retrieves data from both database and server. Deep Map (Malaka and Zipf, 2000) was an early and complex location-based service providing intelligent guidance to tourists. The underlying architecture was agent-based, and components such as the routing agent or the presentation planner communicated over a shared message bus.

On a more abstract level, Hightower et al. (2002) introduced a layered approach for different positioning systems, which they termed the 'location stack'. It is inspired by similar models in the networking domain and consists of a set of layers that build upon one another. From the bottom to the top, the sensor layer deals with low-level hardware and raw data values. The measurements layer combines sensor data to derive location information such as distances or angles. The fusion layer determines the location of objects, and the arrangements layer provides information about spatial relationships between objects. The contextual fusion layer combines location information with other contextual information, e.g. to detect states. The activities layer is concerned with semantics and application-specific states, while the intentions layer deals with user needs and goals.

The example systems and the abstract architectures for LBS discussed above cover a broad range of perspectives and propose different models to conceptualize and build a service that takes into account location. One aspect that is not covered much (if at all) is the question of how location information is managed after the position of the user/device has been determined (e.g. by a set of sensors such as a GPS receiver). Few, if any of the proposed approaches consider how this information is stored and retrieved, how it can be accessed and what should happen with it 'over the long run'. This aspect is however quite central, in particular when considering privacy, which we will discuss in the following section.

2.3 Location Privacy

In order to receive the full benefits of a location-based service, users have to share location data, i.e. where they are or where they have been. Such location data is quite sensitive as it reveals the current physical location of users, and if disclosed would thus pose a serious threat to their privacy and safety. For example, attackers could use this information to either track them down or to exploit their absence, e.g. to break into their home while they are away. Historic location data incurs further privacy threats: attackers can, for example, use it to predict behavior (e.g. to waylay victims) or to infer information about people (e.g. where they live and work or who they know). Even though not all users are aware of these issues, the sensitivity of the location information incurs challenges and difficulties in the process of LBS adoption by users (Xu and Gupta, 2009; Zhou, 2011).

Privacy as a concept has many facets (Council et al., 2007), and different definitions have been proposed—from the classic "the right to be left alone" (Brandeis and Warren, 1890) to "choose freely under what circumstances and to what extent" people share information about themselves with others (Westin, 2003). Location privacy can thus be understood as privacy relating to the location information of a person, i.e. "a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others" (Duckham and Kulik, 2006). Beresford and Stajano (2003) define location privacy along similar lines as "the ability to prevent other parties from learning one's current or past location" (Beresford and Stajano, 2003).

In order to appreciate the importance of location privacy, it is important to understand the risks and threats associated with leaked location data. This is also the first step for exploring possible countermeasures to the identified threats and risks. The rapid proliferation of LBS has resulted in the collection of large amounts of location data, which, in turn, has enabled the analysis of movement patterns. This analysis, if applied by an attacker, is one of the most discussed threats associated with

leaked location information (Krumm, 2009). It has been shown that a broad range of sensitive user-related information can be extracted from analyzing movement patterns. This includes the identity of the user, their (home) address, individual (points of) interests as well as significant events (e.g. strikes or protests) that a user participated in (Hoh et al., 2006; Patterson et al., 2003).

A related issue resulting from large-scale collection of location data is dataveillance, "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" (Clarke, 1988). Key privacy risks associated with dataveillance (Abbas et al., 2015) are the loss of control, (continuous) monitoring, identification, social sorting, and profiling. In general, threats linked to location data have the potential to "disclose a great deal about the movements of entities, and hence about individuals associated with those entities" (Clarke and Wigan, 2011). When exploited in attacks, these threats may cause psychological, social, and economic harm (e.g. loss of control over one's life, social embarrassment, financial damage) to individuals citepclarke2011you. Although many attacks depend on access to recorded (past) location data, the way in which location data is managed has not received a lot of attention.

In order to neutralize these and other threats to (location) privacy and to counter attacks, research has identified a number of general methods to protect privacy. One of the most common methods to secure data in general (and thus location data in particular) is encryption. Encryption is platform and service agnostic and can be applied to secure data. As a key area of cryptography, encryption provides data security through hashing and secret communication (Balogun and Zhu, 2013). While cryptography is considered as an essential and necessary aspect to secure communication, it is not sufficient by itself unless its deployment and implementation are managed adequately (Keßler and McKenzie, 2018)).

In the context of location data and the associated threats, Duckham and Kulik (2006) discuss further measures for privacy protection. Regulatory strategies are a promising approach, where the government defines rules on the use of personal information, for example by passing laws that are binding for LBS providers. A second option is the use of privacy policies, which are trust-based agreements between individuals and whomever they are sharing their location data with. Another generally applicable method is to rely on anonymity. For example, a user might use a pseudonym instead of their real name or create ambiguity by grouping with other people. Finally, it is also possible to use obfuscation, which reduces the quality of location data and thereby prevents attackers from easily learning where exactly a user is located. When applied sensibly, all these methods as proposed by (Duckham and Kulik, 2006) can be implemented without compromising the quality of the LBS.

As a practical example of a privacy through data management implementation, Stroeken et al. (2015) developed a privacy preserving location-based service called Zone-it, a virtual notice board which permits users to have location-based interaction in self-zoning areas and under certain categories. The service places offers

and requests with their exact coordinates on a map. Users can find offers and requests based on their interest and location (zone). After a match is found, the message disappears. Zone-it is a social media service, which shifts the focus from person-based (e.g. Facebook) to goal-oriented communication (Stroeken et al., 2015). On a more technical level, several of the approaches listed above have successfully been implemented. Examples in this area include work by (Krumm, 2009); (Krumm, 2007), where computational countermeasures to mitigate threats are discussed including anonymity, spatial-temporal degradation, specialized queries, spatial cloaking, noise, and rounding. Other countermeasures proposed at this level are the use of a trusted third party, which improves location privacy by serving as an intermediary between providers and users of a location-based service (Mohamed F Mokbel et al., 2006). This intermediary can then employ various strategies, for example dynamically adjusting location quality based on the number of nearby users. A similar approach is the use of mix zones (Beresford and Stajano, 2003), which are spatial areas inside which all clients of a location-based service stop sharing their location with the service provider and also change the pseudonym they are using. This makes it difficult to track individuals when they leave a mix zone. Most of the countermeasures discussed above work based on the assumption that location data is perpetually stored. The role of location data management and its impact on location data privacy are not considered explicitly in the cited papers. Due to the increasing importance and practical relevancy of privacy, Cavoukian (2010) proposed to consider privacy from the start, i.e. the design stage. Their 'Privacy by Design' (PbD) approach describes general principles and essential steps towards realizing better privacy protection in all type of information systems. The goal of PbD is to secure the privacy of individuals by providing them with control over their information (Cavoukian, 2010). For this purpose, the author defines seven basic principles that should be followed when designing an interactive system to ensure that the resulting system respects the privacy of its users:

1. proactive not reactive: rather than wait for privacy risks to occur, such risks should be anticipated and prevented from materializing.

2. privacy as the default setting: the default behavior of a system should be such that the privacy of its users are automatically protected—no prior user action is required.

3. privacy embedded into design: rather than 'patching' a system with some privacy-protection measures, privacy-related functionality should be considered as an integral part of the system and be realized without interfering with its overall purpose.

4. full functionality: unnecessary trade-offs (e.g. security vs. privacy) should be avoided and all legitimate requirements should be realized ("win-win").

5. end-to-end security: all data collected in the system should be protected by strong security at all stages of its life cycle (from creation to deletion).

6. visibility and transparency: all parties involved in the provision of a service and the running of the corresponding system, should expose their practices, policies and technologies so that they can be independently verified.

7. respect for user privacy: the interests, needs, and preferences of users should be considered first and foremost to ensure a user-friendly privacy-preserving system.

While the Privacy by Design approach in principle can be applied to LBS, it is not clear how it could be folded into a location-based service and how it can be used to make existing LBS more privacy-aware. In addition, the issue of managing location data is only implicitly covered and deserves a more thorough analysis due to the role historic location data plays in enabling different types of attacks. In the following section, we therefore propose a conceptual model to facilitate location Privacy by Design, and we introduce the concept of ephemerality of location data as a fundamental approach to realize Privacy by Design in the context of LBS.

2.4 Location Privacy by Design

Service and content providers of LBS are collecting location data from users and are usually storing it for a substantial period of time (Sathe et al., 2014). The rationale for storing the data is manifold. Depending on the country, there may be legal requirements to keep the data for at least a certain amount of time. Being able to analyze historic location data might also provide insights that can help to improve the service. Finally, historic location data also allows for deep profiling of the users, and such profiles constitute a commercial value, such as targeted advertising. From a user's perspective, in particular, the latter use can be perceived as an unwanted intrusion of their privacy.

By default, many LBS rely on a number of different databases for retaining and maintaining various types of data such as service-specific content data, digital map data, or user location data (Lee et al., 2005). These databases frequently are accessed remotely on an as-needed basis and are usually under the control of the service provider. Based on a sample of commercial LBS, the number of LBS that are self-contained on a mobile device is relatively small (e.g. navigation systems with

local map databases to avoid roaming charges while traveling abroad). Research investigating how location data is stored is mostly focusing on technical challenges relating to, for example, handling large amounts of spatio-temporal location data or increasing system performance by optimizing access to location data (Mohamed F. Mokbel et al., 2003). In the light of the various privacy threats discussed above, it makes sense to look at location data management not only from a technical perspective but also from the perspective of how it affects privacy. This aspect, however, has not received much attention in literature. When looking at existing architectures of and models for LBS such as Kivera (Schiller, 2004) or the location stack (Hightower et al., 2002), we can observe that privacy protection for location data is not an inherent part of these models. As discussed in the previous sections, there are a number of approaches to protect location privacy but these are frequently either external to the LBS, e.g. as a trusted third party (Mohamed F Mokbel et al., 2006), or not integrated into the architecture of a location-based service, e.g. the mix zones proposed by (Beresford and Stajano, 2003).

In order to describe more clearly how location privacy protection can be integrated into a location-based service, we propose a conceptual model (see Fig. 1) that facilitates applying existing methods for privacy protection as integral parts of a location-based service. In addition, the model provides means to explicitly consider how location data is managed and how strategies for privacy protection in this context can be realized. It also captures how the configuration of location privacy settings can be exposed to users of a location-based service without requiring thorough modifications of the internal core logic of a service. The model describes how a location-based service interacts with the world and provides a user with a service while explicitly considering location privacy. A set of sensors observes the world and provides information about it, in particular, location data and context data. While the former refers mainly to the position of a user, the latter includes aspects such as environmental factors, the time of the day or the current task of the user. Both types of information are usually stored for later perusal by the service (in a location data storage and a context storage). They are also needed for processing by the core logic of the location-based service. This part encapsulates the main functionality of the location-based service, for example, routing algorithms for a navigation service, or means to retrieve real-time traffic data. This component also interacts with both the location data storage and the context storage, i.e. to retrieve information (e.g. historic location data to carry out dead reckoning) or to update it (e.g. to set the current task of the user to navigation after directions have been requested by the user).

The location privacy management component (LPM) is strongly connected to the location data storage in order to implement various privacy protection measures. It observes and controls the location data storage according to the rules and procedures defined by the designers, developers and/or users of the location-based service. In order to address the location privacy issues, it can actively control the

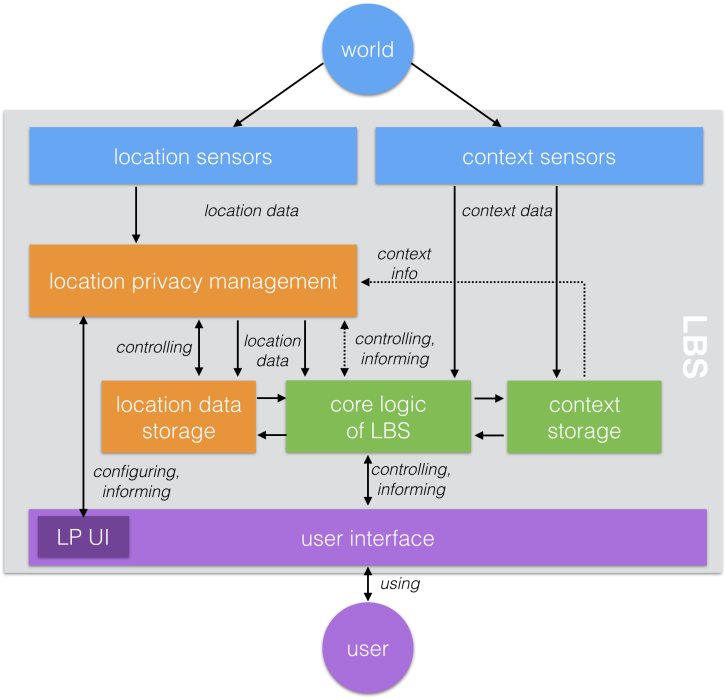


Fig. 2.1: Conceptual model for integrating location privacy management into a location-based service

data storage process. For example, it can reduce the quality of location data received from the sensors prior to passing it on to the location data storage or the core logic of the location-based service along the lines of the concept underpinning Caspar (Mohamed F Mokbel et al., 2006). From the perspective of the Core Logic, only the provider of the location data is different compared to a more traditional architecture, where it receives location data directly from the sensor component. Users of the location based service rely on a user interface (UI) to control the location-based service and receive information from it. The user interface can also incorporate a location privacy user interface (LP UI), which enables users to directly access the LPM in order to inspect how location privacy is managed and to configure it according to their preferences and needs. Providing a component which separately addresses the user interface design and options for LBS users with the goal of increasing their control over their location privacy can be a suitable approach to realize standardized privacy controls at the UI level.

The integration of the LPM and its interaction with the other components of a location-based service facilitates different ways to build a service that takes into account location privacy. In a legacy system, the LPM basically corresponds to a forwarding mechanism that forwards all location data directly to the location data storage and the core logic. A first step towards more location privacy would be to introduce a set of simple rules that the LPM uses when deciding what information to pass on to which component and at what granularity. An example of a rule is to reduce the quality of the location data to improve location privacy if the user specifies

this or when the service does not require completely accurate location information to function. A more sophisticated set of rules could also take into account contextual information such as the time of the day and automatically stop providing location information after the working hours of a user are over. Such a rule set could also facilitate the realization of user-driven preferences with respect to location privacy protection (Toch et al., 2010).

The simple approach described above could be integrated into a location-based service without the need to modify the core logic (beyond changing which component provides it with location data). An alternative and complementary strategy that would also not require any changes to existing components is for the LPM to take more detailed control of the location data storage. In this case, the LPM could directly access the location data storage (e.g. using the same means that the core logic employs) to apply various strategies to recorded historic location data. For example, it could continuously monitor the stored location data to ensure k-anonymity (Sweeney, 2002) (e.g. by accessing social networking sites where other people publish their location). This approach also forms the basis for the temporal ephemerality approach introduced in the following section. More sophisticated strategies for protecting location privacy might require more involved interaction between the core logic and the LPM, and thus entail changes to the former. For example, location privacy could be negotiated on a case-by-case basis with the core logic providing a rationale why positional information of a certain quality is required. Conversely, the LPM might inform the core logic component about new location privacy settings requested by the user so that the core logic might change its behavior in response to this. A complementary strategy is to consider the way in which location data is stored. Beyond technical considerations, there are also different options regarding how the system stores location data, where the data resides in the physical world and whom it is shared with. These aspects play a key role in the realization of spatial ephemerality as a means to protect location privacy (as discussed in Sect. 4.2).

In respect to the privacy-by-design principles, the introduction of the location privacy management component thus facilitates addressing location privacy issues from inside the LBS architecture and it supports realizing this in different ways. In addition to simplifying the integration of location privacy protection into legacy systems, the overall model of course also allows for the creation of privacy-aware LBS from scratch. The following two subsections will demonstrate the usefulness of our model further by first introducing the concepts of temporal and spatial ephemerality for location data and then highlighting how these can be realized using the LPM and the model in general.

2.4.1 Temporal Ephemerality

When location data is stored in LBS databases indeterminately, the window of attacks is substantially enlarged: malicious agents have an unrestricted amount of time to obtain access to the location data and carry out attacks on the user's location privacy. As discussed above, historic location data is particularly sensitive as it allows for very deep inferences on users and their behavior. In order to address this key issue of location privacy, it makes sense to consider how long location information is stored.

Rather than assuming that location information is stored, a more fine-grained consideration of the temporal ephemerality of such information can contribute towards better protecting the location privacy of the user. The basic idea of this concept is that all location information can be assigned an expiration date, after which it is deleted. By defining an expiration time and then discarding location data once it has passed, attackers will be unable to use this data for further attacks in the future (assuming that the location data storage was not breached while location data was still in the storage).

The temporal ephemerality of location data can be specified in different ways. It is possible to assign an overall expiration time for all location data, either in relative (e.g. "delete 24 h after recording") or absolute terms (e.g. "delete today at midnight"). Alternatively, a more fine-grained control is possible as well using a set of rules that determines for each individual piece of location data when it should expire. Such rules could take into account various factors such as context (e.g. "delete all location data when I leave my work place") or user preferences (e.g. "delete very precise location data immediately after recording"). The exact way in which temporal ephemerality is realized can be specified by the designer and developers of a location-based service (while designing and building the service) and by the users while interacting with the location-based service.

In our model, the temporal ephemerality of location data can be easily realized by encapsulating the corresponding rule sets inside the LPM. For legacy LBS, this could be achieved in a completely transparent way as outlined above. The only component that would need to be modified slightly is the location data storage as each entry would get an additional attribute (expiration date) to facilitate the timely removal of expired location data. The LPM could then use this attribute to periodically query the location data storage for all entries with an expiration time in the past and to then delete the returned entries.

In addition to better protecting the location privacy of users in general, implementing temporal ephemerality of location data in this way also realizes several basic principles of the privacy-by-design approach for location data. Supporting the idea of being preventative and not remedial by discarding the data from database, the risk of inference attacks will be reduced as there will be no record of data available for attackers after the expiration date. This follows the 'proactive, not reactive'

principle, where “Privacy by Design comes before-the-fact, not after” (Cavoukian, 2010). With regards to the approach and implementation described above, the discarding of location data occurs automatically once the expiration time has passed, thereby realizing the ‘privacy as the default setting’ principle (This behavior could be changed by users, e.g. via the LP UI, should they wish to keep location data forever). Finally, the approach outlined above very strongly connects with the ‘privacy embedded into design’ principle of PbD. By encapsulating the functionality for temporal ephemerality in the LPM, designers can easily design systems that realize the location-based service while respecting location privacy as the other components are largely unaffected. They can focus on the location-based service functionality and relegate considerations about location privacy to LPM and (to some degree) the location data storage. The LP UI then provides an easy way to expose issues related to location privacy to users. The model also facilitates reuse of components: designers can create generic LPM, location data storage, and LP UI components and then use them to create different location privacy-aware location-based service.

2.4.2 Spatial Ephemerality

In the discourse of (location) privacy, many aspects are discussed but the issue of where location information is stored (and accessible) has received little attention. Usually, the underlying assumption is that stored location data can be accessed from anywhere. If, however, such data is only accessible inside a well-defined spatial area, then attackers or their proxies have to be co-present in order to carry out an attack. In analogy to temporal ephemerality for the time domain, the concept of spatial ephemerality refers to location data having a spatial ‘expiration’ zone: location data is stored in a particular area, and only accessible for users who reside inside this area. More specifically, spatial ephemerality entails that all location data is assigned a spatial expiration zone, and once a user leaves the zone for a particular location entry, it is deleted. To put it differently, location data would not leave a particular geographic area (e.g. the area where the location-based service is most relevant or where the user intends to use it) so that an attacker could not use it once a user has left that area - assuming the data was not retrieved while the user was still inside the area. Similar to the temporal case, the spatial ephemerality of location data can also be defined in relative (e.g. “delete location data that is further than 2 km from the current position”) or absolute terms (e.g. “delete location data that is more than 2 km from the city center”). In addition to specifying general rules for all location data, it is possible to define this for individual pieces of location data. The rules encoding spatial ephemerality can also consider various other factors such as context (e.g. “delete all location data inside a 2 km radius around locations that are visited only by few people”) or user preferences (e.g. “delete all location data inside a 2 km radius around my home”). As with the temporal case, the exact way in which

spatial ephemerality is realized can be specified by the designers and developers of a location-based service (during design and development) and by the users (during usage of the location-based service).

In our model, spatial ephemerality could be realized via the LPM to encapsulate the rule set defining the spatial ephemerality of location data. This approach has the advantage of being completely transparent and thus would lend itself easily to making legacy LBS more location privacy-aware. As with the temporal case, it would be necessary to introduce an additional attribute for location data. Consequently, the location data storage component would have to be modified accordingly. This attribute would hold the spatial expiration area of an entry, for example, in the form of a polyline corresponding to the boundary of the area. The LPM could then periodically query the location data storage component with the current location to obtain all entries, which do not contain this location within their expiration areas. The returned entries could then be deleted.

Spatial ephemerality can contribute towards location data privacy by deleting location data based on spatial conditions, and thereby reduce the risk of inference attacks. The proposed model and approach to realize spatial ephemerality of location data also facilitates the application of PbD principles to location data. By geographically limiting the storage of location data and encapsulating the corresponding rules with default values inside the LPM, the 'privacy as the default setting' principle can easily be realized. Similarly, this approach supports the 'privacy embedded into the design' principle. The 'proactive not reactive' principle of PbD applies as well, as location data is systematically deleted before an attack occurs. The considerations regarding the design and development of privacy-aware LBS (ease of improving legacy LBS, concentration of location privacy concerns in the LPM, reuse of components) we discussed for temporal ephemerality (in Sect. 4.1) hold true for spatial ephemerality as well. In order to further investigate how ephemerality can be implemented and used in everyday life, we have started to develop an initial prototype1 based on our pro- posed model. The prototype[1] is a service designed to enable users to share their experiences while visiting or exploring a city (e.g. special events). The application provides a means to share short messages anonymously with people in the same geographic area. In addition, it empowers users to define an expiration time for each message. The system design is implemented to not store any location data of the users or their messages over time. The location data of users is discarded from the system (website[2] or app) as soon as the user leaves the geographic area or when the messages expire. Our next step is to carry out user studies based on this prototype to gain a deeper understanding on how users act when they are given increased control over their location privacy.

[1] 1https://github.com/heinrichloewen/SC-App.
[2] https://github.com/chack05/sc16-ephemeral-lbs-server.

2.5 Discussion

The proposed location-Privacy by Design approach and the corresponding model for LBS as well as the concept of ephemerality offer benefits and are also subject to a number of limitations. The key benefit of the PbD approach in combination with the proposed model is facilitating the realization of location-privacy-preserving LBS. In Sect. 4, we discussed in detail how this can be achieved both for existing LBS that should be made more privacy-aware and during the design of a new LBS from scratch. The benefits of the ephemerality concept include facilitating sophis- ticated privacy-protection without having to substantially modify all of the com- ponents of a location-based service. In addition, ephemerality of location data reduces the amount of storage needed to hold historic location data, and it provides a unified and simple approach to implement legal requirements (e.g. via expiration dates corresponding to the legally required duration of storing data). Considering that LBS can produce a large amount of privacy sensitive data every day, which requires a secure storage and proper treatment to comply with existing law, the ephemerality approach will also not require the system to obtain more servers over time, which may incur financial savings. From the user's point of view, key benefits of the proposed approach and the model as well as ephemerality include an increased level of privacy and a fine-grained control over the user's location privacy.

These benefits also come with a number of drawbacks and challenges. While there are no inherent technical issues preventing the implementation of the proposed ideas, there are potential business-related implications. Location data can have a commercial value for advertisement partners to LBS companies as the collected location data can provide deep insights into the behavior and habits of users. For example, providing tailored advertisements to users based on those insights can be a viable revenue stream for LBS companies, which ephemerality could negatively affect. A key question in this context is if users would be willing to pay for a service with increased privacy and control to compensate for reduced revenues of service providers due to this. With the non-permanent storage of location data also comes the challenge of maintaining the functionality of LBS that rely on forward predictions based on past behavior. Time-limited data storage could pose substantial challenges when making advance analysis of user data. Selecting expiration conditions (both spatial and temporal ones) carefully to ensure optimal service provision would be one way to address this challenge. Another limitation or drawback of the proposed LPM component is the fact that it is still vulnerable to attacks, and may also be subject to new kinds of attacks. While in principle it can reduce the severity of successful attacks aimed at retrieving historic location information (by reducing the amount of data being stored), the attacks can still be applied. In addition, the component may become a target by itself, for example, by introducing rules into the LPM component that counteract user-specified rules.

A consequence and potential drawback of using the ephemerality feature is the loss of data. This can be discussed from a provider and a user perspective. From the provider perspective, data storage allows the information they gather to be used for profiling or categorizing their users for purposes such as targeted advertising. Historical tracks of location data is a commodity that can be sold to other companies to be used for the same purposes. From the user's perspective, the loss of data can also have consequences. By not storing location information, it may not be possible to get user-adapted or a localized service provision. For applications that strongly rely on recorded location data (e.g. Foursquare), the ephemerality feature may severely affect service quality.

In section three, we have listed a number of approaches and solutions developed and proposed to protect (location) privacy in LBS. It is crucial to mention that LPM as a solution is a complementary approach. Our solution can be combined with other approaches such as encryption or anonymization. Privacy is regarded as a multifaceted problem that is challenging to solve with one single solution. Due to this, combinations of different methods and approaches can be advisable and/or necessary in order to protect the privacy of users. In our discussion, we mainly focused on the management of location data due to its importance and potential in the context of realizing location privacy in a location-based service. We did not analyze contextual aspects in detail, which can also have a severe impact on privacy in general. One option to deal with this issue could be the introduction of a context data management component into our model that would operate on contextual data in a similar way as the LPM deals with location data. Another area we did not discuss relates to users and their under- standing of location privacy. The model foresees a subcomponent of the user interface, the LP UI, as a means for users to configure settings related to location privacy and to access information about it. In order to build LBS that facilitate proper protection of the users' location privacy, these user-facing parts need to be further investigated. In particular, there is a lack of knowledge about the user's understanding of location privacy and related concepts and options, and it is also not clear how to best communicate this to users.

2.6 Conclusion

In this paper, we investigated how location privacy can be realized in the context of LBS. In particular, we looked into the role of location data management in the context of privacy preservation. Based on privacy-by-design principles, we then proposed an approach tailored to LBS and defined a conceptual model to facilitate the implementation of those principles. We showed that this model supports the realization of different privacy protection mechanisms and enables an explicit and fine-grained control of location data management in the context of privacy preser-

vation. In addition, we proposed the concept of temporal and spatial ephemerality as a means to improve location privacy in the context of a location-based service, which can both be realized using the proposed approach and model. The conceptual model and ephemerality concept are complementary to existing methods to protect location privacy such as encryption or obfuscation. Though the proposed approach is subject to some limitations, there are several promising options for further research. One interesting and underexplored area relates to the understanding users have of location privacy, related concepts, and options, and to how to effectively communicate these aspects to them. We are planning to carry out user studies to compare different systems to communicate threats and countermeasures and to gain a deeper understanding of (mis)concep- tions about location privacy. The LP UI component will serve as a platform to facilitate this line of research. A complementary direction for future research relates to the concept of spatial ephemerality. Here, we plan to investigate how opportunistic information sharing can enable spatial ephemerality at the level of the location data storage and/or the core logic of a location-based service. This line of work will rely on the LPM component to realize and to test the prototypes in realistic settings.

3

Privacy theory in practice: Designing a user interface for managing location privacy on mobile devices

> *To be left alone is the most precious thing one can ask of the modern world.*
>
> — **Anthony Burgess**
> (Homage To Qwert Yuiop: Essays)

This chapter was published in preparation for the Journal of Location Based Services TLBS as Ataei M., Degbelo A., Kray C. (2018) "Privacy theory in practice: Designing a user interface for managing location privacy on mobile devices." Journal of Location Based Services - TLBS. https://doi.org/10.1080/17489725.2018.1511839.

Disclosing the current location of a person can seriously affect their privacy, but many apps request location information from users to provide location-based services. Simultaneously, these apps provide only crude controls for location privacy settings (sharing all or nothing). There is an ongoing discussion about rights of users regarding their location privacy (e.g. in the context of the General Data Protection Regulation - GDPR). GDPR requires data collectors to notify users about location data collection processes and to provide them with opt-out options from these processes. Taking these two characteristics of notice (awareness) and control into account, we propose a set of UI controls for fine-grained management of location privacy settings based on privacy theory (Westin), privacy by design principles and general UI design principles. The UI notifies users about the state of their location data sharing and provides controls for adjusting their location sharing preferences. It addresses three key issues: *whom* to share location with, *when* to share it, and *where* to share it. Results of a user study (N=23) indicate that (1) the proposed interface led to a greater sense of control, that (2) it was usable and well received by participants, and that (3) participants were keen on using it in real life. Our findings can inform the development of interfaces to manage location privacy.

3.1 Introduction

Location information is critically important for a number of useful services such as wayfinding, place-based search, geographical data mining, location-based advertising and map-based visualisation of phenomena. While these services use such information (mostly) to the users' benefit, location sharing also comes with several threats (e.g. identification-, tracking- and profiling threats (Fawaz and Shin, 2014)).

Threats linked to location data can "disclose a great deal about the movements of entities, and hence about individuals associated with those entities" (Clarke and Wigan, 2011). Thus, current trends in large-scale location data collection have the potential to lead to *dataveillance*, which Clarke (1988) defines as the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons. There are various hazards associated with dataveillance (Abbas et al., 2015) such as the loss of control, (continuous) monitoring, identification, social sorting, and profiling.

Because of these concerns, protecting location privacy in location-based services (LBS) is a crucial matter. Location privacy is defined as the *individual's right not to be subjected to unauthorised collection, aggregation, processing and distribution (including selling) of his location data. It is the right to be protected by the ability to conceal information of whereabouts, which can be derived from personal location data* (Bargiotti et al., 2016). Because of the importance of location privacy, there is an ongoing drive to develop strategies to mitigate risks associated with the exposure of unwanted location data. These strategies include (1) regulatory policies (Duckham and Kulik, 2006), where rules are defined by governments regarding the use and collection of personal data[1], (2) privacy policies, which "are an established principle in legal domains to codify data collection and usage practices" (Langheinrich, 2002), and (3) technical methods such as anonymization, spatial and temporal degradation, specialised queries (Krumm, 2009), obfuscation (Brush et al., 2010; Zakhary et al., 2017), or Mix zones (Beresford and Stajano, 2004). The combination of all these strategies are important to protect the location privacy of LBS users.

In line with Ataei and Kray (2017), a privacy-aware LBS requires three main types of components: sensing components, a location privacy management component, and a user interface component. Each of these components is responsible for addressing privacy issues on a different level. The sensing and management components are predominantly used in the strategies listed above (e.g. anonymisation, obfuscation) to mitigate location privacy at higher levels that do not involve the user; however, the user interface component addresses these issues differently: it allows users to manage location privacy directly. The focus of this article is on managing location privacy at the UI level, similar to that mentioned by Ataei and Kray (2017). In this

[1] A recent example of a regulatory policy is the General Data Protection Regulation (GDPR) which was adopted on 27 April 2016 and will enter into application 25 May 2018, see `https://gdpr-info.eu` (last accessed: April 20, 2018).

context, there are two main issues for the users of LBSs. The first is that they lack control over how they share their location information. Most current apps provide only crude controls for location privacy settings. As Fawaz, Feng, et al. (2015) put it: “the user either enjoys full privacy with no utility, or total utility with no privacy". The second problem is related to the limited amount of information that users receive about the fate of their collected location data. Current practices - in most cases - provide written privacy agreements. This kind of representation is not easy for users to comprehend (D. J. Solove, 2005), so those designing LBS face the challenge of communicating to users what is happening behind the scenes, and users must understand why it is important to protect their location privacy.

In this paper, we are specifically addressing the lack of control problem. The work aims to provide a UI that helps users to manage their location privacy in a more fine-grained manner. The main contributions of this paper are:

- *A set of UI elements*, grounded in existing privacy theories that facilitate fine-grained control of how location information is shared. These features inform users about what is happening to their location data, and then enable them to specify who to share location with, when to share it, and where to share it;

- *Insights into users' expectations regarding location privacy controls*. The experiment we conducted revealed that users want location sharing to be turned off by default and that they prefer changing the accuracy of their location by specifying the spatial area within which their location should be shared;

- *Results of an exploratory study on UI design for location data privacy protection*. For instance, the experiment brought to light that the proposed interface was usable, led to a greater sense of control, and that participants were keen on using it in real life.

The remainder of this paper is structured as follows. We first review previous work from related areas. We then introduce our theoretically grounded UI to provide users with fine-grained control over how they share their location. In the following section, we report on the user study we carried out to evaluate the developed UI and to gather insights into location privacy preferences and usefulness of proposed UI controls. We then discuss the results we obtained as well as their implications and limitations. The paper concludes by summarising our main contributions and pointing out promising future work.

3.2 Related work

UI design for location privacy should be informed by users' perceptions of privacy in general, consider the peculiarities of location privacy, and incorporate suitable user interface elements. We briefly review previous work in these three areas.

3.2.1 Users' perception of privacy

J. Lin, Liu, et al. (2014) provided empirical evidence that a unified default setting cannot satisfy all users' privacy preferences. Their study also suggested four types of users: the (privacy) "conservatives", the "unconcerned," the "fence-sitters," and the "advanced users." The (privacy) "conservatives" do not like their private resources used by any external party; the "unconcerned" feel comfortable disclosing their data to third-parties in most cases; the "fence-sitters" are neutral (i.e. neither comfortable nor uncomfortable) with respect to giving information to third parties; and the "advanced users" have a nuanced understanding of the sorts of usage scenarios they should be concerned about. In addition, J. Lin, Liu, et al. (2014) indicated that preferences of privacy pragmatists in the sense of Westin (see Kumaraguru and Cranor 2005a for a definition of privacy pragmatists) can be captured using "fence-sitters" and "advanced users." The study in (Chanchary and Chiasson, 2015) confirmed differences in users' sharing willingness based on privacy attitudes (with Westin's privacy fundamentalists being less willing to share information including location information).

In addition, participants reported that they would be more willing to share if given control mechanisms to specify which information is collected by whom. In sum, there are different types of users, most of whom are willing to share information if appropriate control mechanisms are readily available.

Regarding users degree of privacy concerns, Kang et al. (2015) pointed out that past negative experiences trigger more secure online behaviour and a greater level of concern. They suggested that designers provide a "privacy indicator" for people's Internet activities that *shows them who can see what information*. Besides, Chin et al. (2012) observed that users are more concerned about privacy on their smart phones than their laptops. The results from these two studies indicate that there is a need for *visual privacy cues* on smart phones. Ideally, these should also cater for the four types of users identified by J. Lin, Liu, et al. (2014).

3.2.2 Privacy and location sharing

Other studies have also investigated privacy considerations with respect to location sharing. These touched upon users' willingness to share their location, the moti-

vations and factors influencing location sharing, and the use of more controls for location privacy management. Tsai, P. Kelley, et al. (2009) primarily investigated willingness to share, and observed that users' privacy concerns can be reduced through feedback (i.e. providing users with information about when and by whom their location information has been viewed). In addition, Tsai *et al.*'s study illustrated that people are willing and able to use rules to control access to their location information.

Regarding motivation for sharing, Patil et al. (2012) found three main motivations for location sharing (a) to connect and coordinate with one's social and professional circles; (b) to project an interesting image of oneself, and (c) to receive rewards offered for 'checking in'. Consolvo et al. (2005) identified three main factors that contribute to users' decision of whether and what to disclose regarding their location: who is requesting the location information, why that person is requesting it, and what would be most useful to the user. Finally, users' desire to use more controls on location sharing has also been investigated. Participants in Benisch et al. (2011)'s study reported being comfortable with (the possibility of) sharing their location using time- and location-based rules. Generally, more complex location privacy settings lead to more sharing, and may make services more valuable (see Benisch et al. 2011). However, the proliferation of choice in a privacy context may also, as Korff and Böhme (2014) observed, bring about less user satisfaction. For this reason, they recommended that designers follow choice minimising principles, and weigh the necessity of introducing additional privacy options. This recommendation was taken into account while designing the user interface presented in Section 3.3.2. While observations from their study led Chin et al. (2012) to emphasise that researchers' strong emphasis on location privacy may be misplaced, the importance of location privacy cannot be denied. For example, respondents in (Patil et al., 2012) identified having to face undesired social consequences as a result of unintended location disclosure. It is thus crucial to "explore effective ways to define and manage access based on audiences, locations, and specific times and situations" (Patil et al., 2012). In this paper, we tackle this issue specifically from a user interface perspective.

3.2.3 Location privacy management through user interface design

While technical solutions to manage location information are a prerequisite for building LBS that can protect location privacy (e.g. Olumofin et al. (2010) and Narayanan et al. (2011)), this is not sufficient. There is also need to address location privacy at the user interface level. Previous work on UI design for LBS has mainly focused on comparing the performance of different user interface designs. For example, Rinner et al. (2005) compared two UI designs for location-based decision services

and concluded that the MCE (multi-criteria evaluation) method, the degree of detail in criterion weighting, and the availability of user-defined criterion standardization are important parameters for easy-to-use location-based decision services. Stroeken et al. (2015) proposed two interfaces to visualize spatial and temporal information about events (e.g. cultural happenings) of interest to a user: the CLOCK-view and the NEAR-view. The CLOCK-view enables the display of spatial and temporal information about events in the form of cones placed on a dial. The NEAR-view places events in a two-dimensional space with time as abscissa and distance as ordinate. The CLOCK-view was perceived as counter-intuitive by most test-users, while the NEAR-view seemed easier to interact with. Church et al. (2010) compared map-based, and text-based interfaces for location-based search services on mobile phones. They observed that users preferred the text-based interface when *consuming* information while favouring the map-based interface when *seeking* information related to a specific address. They concluded that the choice of interfaces depends on three factors (i.e., personal preferences, information need and situational context) and recommended that location-based search tools should support both text-based and map-based interface modalities. Useful UI elements for the design of map-based LBS were mentioned in (Gartner, 2004). These included overview maps, automatic scrolling, the combination of maps and spoken/written text for communicating route information.

There is also work on fine-grained controls for adjusting privacy. Epstein et al. (2013), for example, developed an interface that allows users to modify the data collected about them (e.g. deleting part of the data). Their focus was only on step activity sensed by a FitBit[2] pedometer, but their simple UI approach could be applicable in the context of location privacy. Another example of fine-grained configuration was Loccacino by Toch et al. (2010). Loccacino facilitated location sharing by allowing users to set up privacy rules and access privacy management functionality through a location sharing app in the context of social network (i.e. Facebook), and only with Loccacino users. While our approach in this paper has some similarities to Loccacino regarding the controls (i.e. both approaches provide possibilities of defining location sharing restriction based on group (who), time and location), there are some fundamental differences. For example, Loccacino provides the option of specifying with whom a user wants to share his or her location information, this is limited to the user's social network group; conversely, our approach defines a category of people that users can enable or disable access to location sharing information based on his or her social intimacy level, from significant other to unknown parties. In addition, our focus is to explore ways of designing UI based on privacy and design theories on the OS levels while Loccacino's purpose was to work as a tool for studying user preferences without any specific emphasis on the design of UIs.

While some standard UI elements for LBS have emerged on commercial plat-

[2] http://www.fitbit.com/

forms (e.g. regarding the depiction of and interaction with points of interest via standardized mappings or privacy controls in social networks), general UI principles for designing user interfaces for location-based services have not been proposed and evaluated yet. Consequently, such guidelines or standard UI elements still do not exist for the control of location privacy. From the previous work presented above, we can infer that there is currently a need for visual cues to communicate privacy to users. What's more, these visual cues should provide more options to the users with respect to managing their location privacy.(In fact, the lack of choices was identified in (Schaub, Balebako, et al., 2015) as one of the reasons why privacy notices are ineffective.) Furthermore, the controls should be easily accessible from the main page of applications. These gaps are addressed by the design of the UI presented in the next section.

3.3 A User Interface for Managing Location Privacy Settings

Iachello et al. (2005) provided some early guidelines for the design of location-sharing (social) applications. The guidelines cover issues such as personal boundary definition, deception, and denial,as well as group vs. individual communication, but they did not review UI considerations. Likewise, Schaub, Balebako, et al. (2015) presented some best practices for privacy notice design; such best practices included aspects such as diversity of audiences, systems' input and output modalities, and layering of notices, but again they did not discuss the peculiarities of location privacy. Since there is a lack of guidelines specifically tailored to UI design for location privacy, this work resorted to a combination of privacy theory (Westin), privacy by design principles and general UI design principles while developing the user interface (see Figure 3.2).

3.3.1 Theoretical grounding

There are a number of general UI design rules and principles that can be applied to any user interface, but these are not tailored to specifically address UI design for location privacy. We, therefore, developed a model that combines key concepts that are relevant in this context. It consists of three circular layers (see Figure 3.1). At the heart of the model (red circle) are the four states of privacy according to Westin's theory (Westin, 2003). The second circular (blue) band contains the seven principles of privacy by design based on Cavoukian's work (Cavoukian, 2010). The outmost circular layer (green) represents Shneiderman's eight golden rules of interface design (Shneiderman, 2010).

In the following paragraphs, we explain these three layers in detail and the rationale behind choosing them for the design of UIs for location privacy.

The first step for addressing privacy issues is to have a well-defined description or concept of privacy (Stephen T. Margulis, 2011). Privacy is a complex notion, since there are a number of factors and dimensions which can vary based on culture or context. The perception of privacy can also be subjective and differ from one individual to the next. Thus, it makes sense for designers or developers to carefully select the most fitting definition according to the purpose of the system being built.

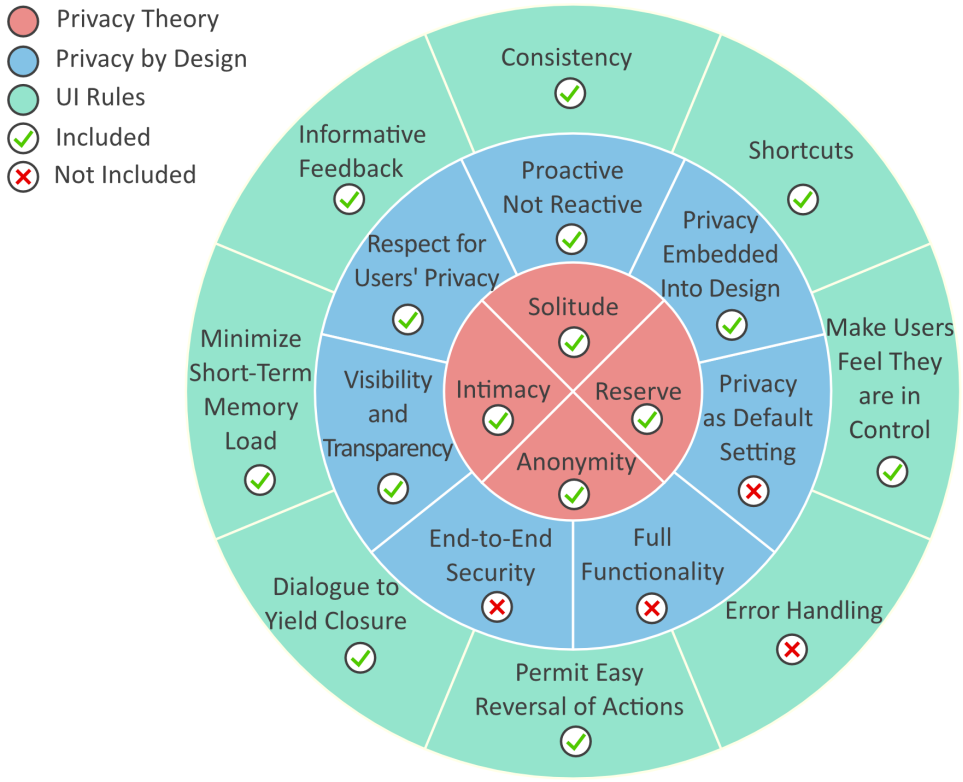


Fig. 3.1: Combined theories and principles guiding the design of the proposed UI for location privacy.

Westin defines privacy "as the claim of an individual to determine what information about himself or herself should be known to others" (Westin, 2003). It is also relevant to consider the use and circumstances for which this information is obtained by others. According to Westin, there are three levels to address privacy in a society: the political level, the socio-cultural level and the individual level. Privacy at a political level is based on a society's political philosophy. For instance, there is a difference between authoritarian societies and democracies regarding how much value they attach to the private sphere in relationship to public order. Privacy at the socio-cultural level refers to "the real opportunities people have to claim freedom from the observation of others. [..] In this sense, privacy is frequently determined by the individual's power and social status" (Westin, 2003).

Individual privacy, which arguably is the most relevant of Westin's levels (Westin, 2003) in the context of location-based services, was chosen as the core of our model for two main reasons. First, Westin's notion of individual privacy focuses on the level of individuals' relationships so that users can relate the concept to their everyday experience when directly interacting with other people. (For example, the level of closeness or trust to others is a fundamental measure to decide to what extent one wants to disclose information about oneself to others). Second, the four states defined on this level (solitude, intimacy, reserve, anonymity) are familiar to average users and thus lend themselves well to being translated and visualised on the UI level.

Individual privacy consists of four basic states: solitude, intimacy, anonymity and reserve. *Solitude* refers to the freedom from being observed by other parties. *Intimacy* means being in a position to become a member of a small group (including one or just two people), who maintains a close, honest and relaxed relationship. Anonymity refers to not being subjected to surveillance in public [3] Finally, *Reserve* relates to the freedom of limiting what information about a person is disclosed to others (Stephen T Margulis, 2003). These four states of individual privacy clearly relate to what users of location-based services may want to achieve or maintain while they make use of such services. Therefore, it makes sense to include them at the centre of the model for the design of UIs for location privacy (red circle). All four states are also reflected in the UI design presented in Section 3.3.2.

In addition to the core privacy states that are relevant to the individual, the design process itself needs to be considered in more detail. Instead of retrofitting privacy-related UIs onto an existing system, Cavoukian (Cavoukian, 2010) and others have argued strongly for considering privacy from the start, i.e. from the very first stages of design and development. Cavoukian coined the term 'Privacy by Design' (PbD) and detailed seven basic principles to ensure better privacy protection in information systems (Cavoukian, 2010). *'Proactive not reactive'* refers to the principle of anticipating and preventing privacy risks rather than waiting for them to materialise. *'Privacy as the default setting'* relates to how a system deals with privacy by default: this principle calls for full privacy protection without the need for any initial user interaction. *'Privacy embedded into design'* means that privacy protection should be integrated into a system's design without interfering with its general purpose. *'Full functionality'* refers to the principle of avoiding trade-offs such as security vs. privacy while realising all functional requirements of a system. *'End-to-end security'* calls for strong security measures at all stages and for all data collected in the system (from creation to deletion). The *'visibility and transparency'* aspect calls for all parties involved in the running of a system/service to fully disclose

[3] Definitions of anonymity from the technical perspective e.g. *"Anonymity: use a pseudonym and create ambiguity by grouping with other people*" (Krumm, 2009) or *"Anonymity of a subject from an attacker's perspective means that the attacker cannot sufficiently identify the subject within a set of subjects, the anonymity set*" (Pfitzmann and Hansen, 2010), are compatible with Westin's concept of anonymity.

how they operate and what policies and technologies they use. The *'respect for user privacy'* principle states that users' interests, preferences, and needs should be prioritised to ensure a privacy-preserving and user-friendly system. We included all seven principles on the second level of our model (blue circular band). In the UI design process we were able to include four out of seven principles (marked by green checked dots in Figure 3.1). The final key consideration regarding UI design for location privacy we needed to capture in our model is how information is visualised and how people interact with these visualisations. Addressing this aspect on a general level, Shneiderman proposed the "Eight Golden Rules of Interface Design" (Shneiderman, 2010), which are meant to be relevant for all interactive systems. These rules are detailed in (Shneiderman, 2010) and include (1) strive for consistency, (2) cater to universal usability, (3) offer informative feedback, (4) design task flows to yield closure, (5) prevent errors or offer error handling, (6) permit easy reversal of actions, (7) make users feel they are in control, and (8) minimise short-term memory load. These eight rules form the outermost layer of our model (green circular band). For the UI design presented in Section 3.3.2, we applied seven rules (marked with green checked dots in Figure 3.1).

Thus, the proposed model with three layers includes core privacy states of individual users, privacy by design principles, as well as general rules for the design of interactive technology. When designing a UI for location privacy, e.g. to configure individual settings, developers and designers can use this model to analyse and describe their UI designs. Additionally, it can serve as a tool to assess if a UI follows the principles laid out in the literature regarding the key aspects of UI design for location privacy. In our case, we used this model to design the UI presented in the following subsection, aiming to provide users with fine-grained and easy-to-use controls to manage location privacy.

Complementary to existing theories on privacy and privacy-by-design as well as to general UI guidelines, it also makes sense to consider how user interfaces that manage location privacy settings can be integrated into a location-based service. Ataei and Kray (2017) introduced a conceptual model that allows for integrating location privacy control into a location-based service on an architectural level. They proposed three generic components to make location-based services more privacy-aware: location privacy management, location data storage and location privacy UI. The latter component is meant to inform users about location privacy and provide means to configure privacy settings. The user interface for managing location privacy settings that we introduce below could be part of such a generic UI component.

3.3.2 UI Design

Based on the analysis of relevant theories and by using the core elements of our model, we designed a UI to communicate and manage location privacy settings for

location-based services on mobile devices. The UI we designed is brought up by tapping the circle depicting the user's current location on the map (see Figure 3.2a, top right). When it is called up, it presents three circular icons that represent the key dimensions of location privacy (see Figure 3.2a). These enable users to control *when* (clock icon) to share location information, *with whom* (person icon) and *where* (ruler icon). Tapping any of those icons in the UI allows users to manage the corresponding dimension in detail. The time- and distance-based controls operate in the same way. When users tap either of them, they are presented with an input box inside the corresponding icon (see Figure 3.2c), where they can enter a time in minutes or a distance in meters. These values are then determine for how long or within which radius around the users' current position location tracking is suspended. Once users enter a value for either type of control, the corresponding icon turns green to indicate that this restriction is now active (see Figure 3.2d).

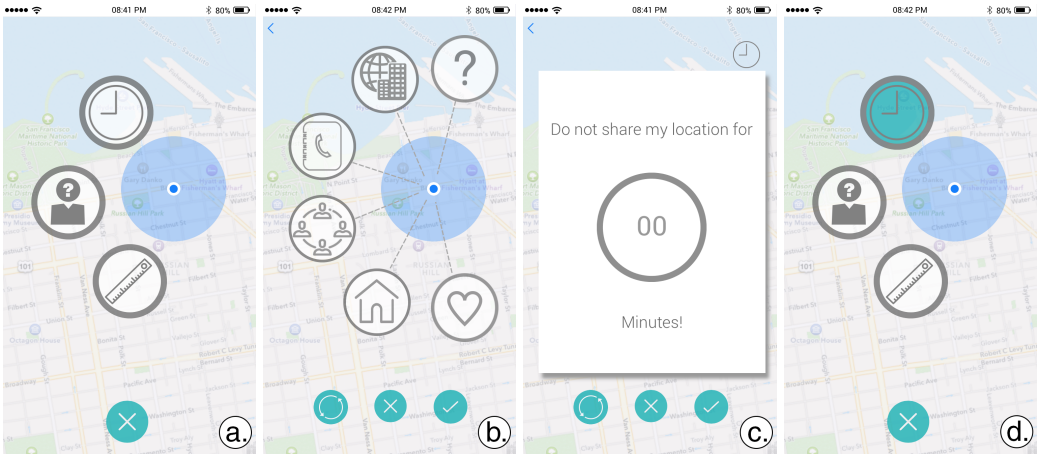


Fig. 3.2: User interface for managing location privacy settings, from left: a) Main UI, b) UI for whom to share, c) Adjusting time restriction, d) Visualised feedback on activated time restriction.

Figure 3.2b depicts the interface for managing with whom location information is shared. It depicts six different parties based on our literature review and current practice in mobile applications providing location-based services.

The selection of concepts and the design of the visual elements was guided strongly by Westin's description of individual privacy. He states: *"In these states of privacy, the individual's needs are constantly changing. At one moment, a person may want to be completely alone, in down time. At another moment, individuals may want (or even desperately need) the companionship or sustaining presence of an intimate friend ... such changing personal needs and choices about self-revelation are what make privacy such a complex condition, and a matter of personal choice" (Westin, 2003, page 433)*. In order to address this complexity, we defined the controls to provide the possibility of supporting each of the individual's privacy states. All three controls provide users with an opt-out option from sharing their location information, meaning that all three controls (i.e social, temporal and spatial) support Solitude (i.e. freedom

from being observed by other parties) and Anonymity (i.e. not being subjected to surveillance in public). To support Intimacy (i.e. maintaining a close, honest and relaxed relationship), we defined different levels of information disclosure based on each individual's relation to others (i.e. whom to share with). All the provided controls also support Reverse (i.e. freedom of limiting what information about a person is disclosed to others). While each of the controls covers different ways of opting out from sharing location information or being tracked, all support the four states of individual privacy (Westin, 2003).

Previous work (e.g. Assad et al. 2007; Tsai, P. G. Kelley, et al. 2010; Toch et al. 2010) has consistently identified close friends and family as important stakeholders in location sharing activities for users. We, therefore, introduced two UI elements to represent these two groups, i.e. the 'home icon' for family and the 'connected people icon' for close friends. We also included a 'heart icon' to represent a user's significant other, to add an intimate level control, distinct from friends and family. Recent trends in LBS facilitate such person-to-person connections, for instance, transmitting heartbeats to a significant other through bracelets[4].

Many current mobile applications also request access to the user's address book, which is why we included 'phone book icon' to represent people in a user's list of (known) contacts. App producers or service providers are also indispensable stakeholders in location-based services who usually request access to location information. Therefore, this group is represented in the UI through the 'globe plus building icon'. Finally, we added a 'question mark icon' to represent unknown companies, since some service providers sell location information to third parties.

In general, tapping either of those icons toggles between sharing and not sharing location information with that specific group (i.e. the icon and its connection is greyed out to show location information sharing has been stopped). Besides the six social controls above (which help to specify "who to share with"), time and distance controls were also designed based on the four states of Westin's privacy theory. These controls allow users to opt out of being observed by others (i.e. solitude) and limit their personal information disclosure (i.e. reserve) along with giving users the possibility of not being subjected to surveillance in public spaces (i.e. anonymity).

Some cases have been reported where location data collection, the location data processing and secondary use of collected data happened without the users' knowledge (Claburn, 2017). Notifying users about these processes is necessary and frequently required by regulations but it is problematic when such notices are limited to the general terms and conditions or privacy policies. In such cases, users may only have a general understanding that their location information is going to be shared with the provider and maybe others, but it is difficult for them to figure out what exactly is happening to their shared location data. In order to avoid this issue, we applied several measures in our UI design such as providing fine-grained opt-out

[4] `http://www.littleriot.com`, accessed June 7, 2018

facilities (described above), and providing continuous access to location privacy controls. From privacy by design principles (Cavoukian, 2010), we have applied four out of seven principles in the design process of our UI: (1) proactive not reactive, by preventing privacy risks from materialising rather than waiting for them to occur; (2) privacy embedded into design, by integrating privacy-related functionality into the system; (3) respect for users privacy, by developing a user-friendly privacy-preserving system that ensures users' interests, needs, and preferences; and (4) visibility and transparency, by exposing the practices of all involved parties so that they can be independently verified.

The overall design of the user interface follows basic principles from human-computer interaction. The large icons facilitate touch interaction, which is the main means of interacting with mobile devices. The use of icons rather than text aims to increase accessibility as well as usability across different languages and alphabets; these icons also follow a consistent sequence of actions (i.e. first rule of eight golden rules of Shneiderman (Shneiderman, 2010)). The design of icons was borrowed from well-known applications for social networking, which makes them easy to learn. There is also immediate feedback after activating each control, which supports the third rule of Shneiderman (Shneiderman, 2010). Finally, the UI is seamlessly integrated with the standard way of depicting location information on a map, thereby enhancing rather than replacing familiar interfaces.

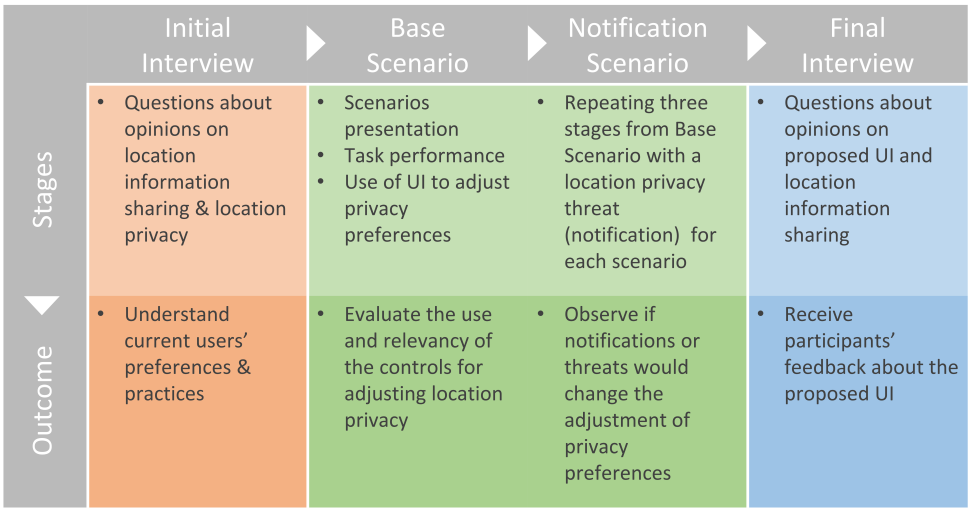


Fig. 3.3: Study overview : four stages of the study process.

3.4 User Study

The goal of the study was to gain insights into users' preferences regarding location privacy as well as to assess the usefulness of the designed UI controls based on our proposed model for location privacy management. This was achieved by analysing the data gathered through an initial interview, two stages of task performances to

observe the use of the controls in different scenarios, and a final interview with general feedback from the participants about the proposed UI design, and their expectations of location-sharing platforms.

Regarding the design of our study, We used an exploratory design for our user study for two reasons. Firstly, there is little prior research on UI controls for location privacy management, which we could rely on to replicate previous study designs. Secondly, exploratory study designs facilitate gaining an initial and deeper understanding of areas that are as of yet underexplored. While the model (Figure 3.1) foresees disabling all location sharing by default, in the study we replicated current practice in current and popular LBS, where sharing location information is enabled by default or during the app installation if the user does not actively disable it. We divided our study design into four stages in order to fulfil our goals (Figure 3.3). The steps followed during each of the stages are detailed in Section 3.4.3. With respect to the type of study conducted, this work opted for a lab-based investigation. It is well known that lab-based and field-based studies have both advantages and disadvantages (Sun and May, 2013). In this work, a lab-based study was chosen because the aim was to explore acceptability issues with entirely new and unfamiliar UI elements. That way, usability issues can be detected and fixed early on - with reasonable effort - before the UI is deployed in the field. In addition, as Sun and May (2013) commented, adding contextual richness to laboratory settings through scenarios and context simulation can contribute to the realism of the experiment while maintaining the benefits of a controlled setting. This was the main motivation for using the five scenarios (to be presented later), and the Immersive Video Environment (IVE) (Delikostidis et al., 2015) (Figure 3.4). The presence of IVE in our study helped us to carry out a study which can be considered as a lab study with rich contextual information, as we were able to simulate different places for participants. Following ethical approval by the institutional ethical review process, we ran the study in our lab during January and February 2017.

3.4.1 Participants

We used online channels (i.e. university mailing lists and Facebook pages for international students) to advertise our study. Each announcement contained general information about the study (location, duration, compensation, and overall goal). 13 female and 10 male participants with an average age of 26 were invited to the lab at our university for the experiment. All 23 participants had a bachelor's degree or higher, the majority of them (15) in an IT-related subject. Also, all participants had prior experience with using smart phones. Most of them owned mobile phones running Android (17) followed by iOS (3) and Windows Phone (3). The participants were compensated with 10 Euros for their time. The total average time spent in each of the sessions of the study was 60 minutes.

Fig. 3.4: Lab study setup - Immersive Video Environment (IVE) - Pilot Study.

3.4.2 Materials and stimuli

The interactive prototype (see Figure 3.2) was presented to users on an iPhone 6 with 4.7" touchscreen. To increase the immersion for users, the study took place in a lab with an immersive video environment (see Figure 3.4). The setup included three large screens that were arranged in a semi-circle around the participant and the experimenter. These screens displayed panoramic photos of the five places referred to in the study: work or school, pub, new city, home, and shopping mall. The presence of the immersive video environment during the lab study allows a greater level of immersion (as Delikostidis et al. (2015) and Loomis et al. (1999) show, for introducing futuristic or fictional scenarios, there are benefits to running lab studies in such environments compared to relying only on the users' imaginations).

3.4.3 Procedure

After welcoming a participant, we first handed out a documentation pack containing the consent form and general information about the study. Participants were informed of the general topic of the study (i.e. location privacy), but they were not provided any specific detail about the purpose, the scenarios, and the possibility of receiving a notification while testing the prototype. We did this in order to avoid priming them in advance about the notifications associated with possible threats to their location privacy. During this time, the participants could ask any questions, which were then answered by the experimenter. Later, we solicited the participants to sign the consent form to initiate the actual study. The procedure we followed consisted of three main parts.

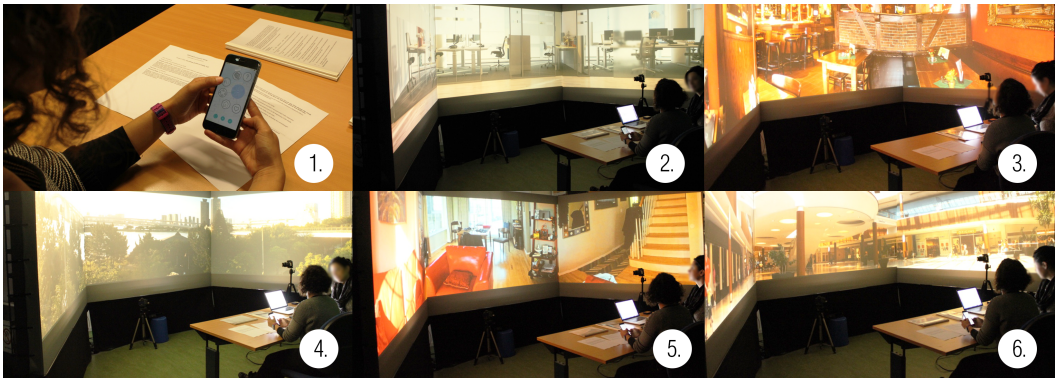


Fig. 3.5: Lab study setup - Immersive Video Environment (IVE) : 1. Participant adjusting privacy settings through UI. 2. Work/school scenario. 3. Pub scenario. 4. New city scenario. 5. Home scenario. 6. Shopping mall scenario.

The first part of the study began by briefing the participant about the subject of the study and details of the procedure (e.g. method for recording data, participants' rights, and expectations). An initial structured interview collected basic demographic information and contained questions about participants' current practices towards managing their location information. During this interview, the experimenter queried participants about their overall perception, their previous experiences (i.e. invasion of digital privacy), and concerns regarding location information and location privacy. The purpose was to understand how much users know about the options they have for protecting their location privacy, not to study their behaviour regarding location data sharing (i.e. find out what they say vs how they adjust privacy preferences).

In the second part, the participants were asked to use the developed prototype. They were given the mobile phone with the pre-installed prototype for location privacy controls. The experimenter then introduced the participants to the controls, by saying that they have the opportunity to adjust location information sharing through these controls in every location-based service that they use during the experiment. The experimenter also explicitly mentioned that the participant's privacy adjustment is not restricted only to these controls, that is, the participants could choose to make no change, use the controls of the prototype or any other setting from the phone (e.g. turning off their GPS) that they would prefer. And users were told they can have access the controls by tapping on the circle on the map or an element like a triangle on the menu while using an application which shares their location information. Besides the general introduction, the experimenter also briefly explained the meaning of the icons from Figure 3.2. Once the interface was clear to the participants, they were informed that they would be asked to imagine themselves in five different places. The experimenter also told them that, by default, their location information is shared with everyone. Furthermore, they were informed that regardless of what changes they applied to their location privacy settings in one place, their settings would be reset once they went to a different place. That is, preferences expressed in one scenario could not be taken in to another scenario

(e.g. location information is always initially shared with everyone at each new place). Finally, all participants were asked to think aloud while interacting with the prototype. Then the five places were presented sequentially while the participant sat side-by-side with the experimenter in the centre of the three screens (see Figure 3.4). For each place, a panoramic picture of the place was shown on the screens. The experimenter also verbally introduced the displayed place by first describing the *base scenario* (see below) and then prompting participants to see if they want to adjust their location sharing setting in the presented scenario. After the base scenario, the experimenter verbally introduced the *notification scenario* (see below) and repeated the process applied in the base scenario. The overall procedure was repeated for all five places. The detailed description of the scenarios is as follows:

- Work / School:
  Base scenario: Imagine that you are at work or school, where you spend most of your time during the day, and your location is going to be shared with everyone. Would you consider changing anything regarding your location information setting?
  Notification scenario: Imagine that you are at work or school, and your location is going to be shared with everyone. All of a sudden you receive a health tip notification reminding you that you have been sitting for a long time and it is time to take 5 min break. Would you consider changing anything regarding your location information setting?

- Pub:
  Base scenario: Imagine that it is weekend and you are going to a pub/bar to visit some friends and eat or drink something. your location is going to be shared with everyone. Would you consider changing anything regarding your location information setting?
  Notification scenario: Imagine that it is weekend and you are going to a pub/bar to visit some friends and eat or drink something. Your location is going to be shared with everyone. The moment you step in, you receive a notification from your insurance company reminding you how bad alcohol can be for your health. Would you consider changing anything regarding your location information setting?

- New City as a tourist:
  Base scenario: Imagine that you are visiting a new city, and you arrive to this spot, and your location is going to be shared with everyone. Would you consider changing anything regarding your location information setting?
  Notification scenario: Imagine that you are visiting a new city, and your location is going to be shared with everyone. The moment you arrive at

this spot, you receive a message from the airline where you got your ticket, suggesting you a good restaurant in this area. Would you consider changing anything regarding your location information setting?

- Home:
  Base scenario: Imagine that you are at home, and your location is going to be shared with everyone. Would you consider changing anything regarding your location information setting?
  Notification scenario: Imagine that you are at Home, and your location is going to be shared with everyone. All of a sudden you receive a notification from a dating website, telling you someone who is not nearby would like to meet you. Would you consider changing anything regarding your location information setting?

- Shopping Mall:
  Base scenario: Imagine that you are in a shopping mall, and even though it is indoors, they have a modern positioning system, so your location is going to be shared with everyone. Would you consider changing anything regarding your location information setting?
  Notification scenario: Imagine that you are in a shopping mall, and even though it is indoors, they have a modern positioning system, so your location is going to be shared with everyone. The moment you step into the mall, you receive a notification from a clothes store that if you go there right now, you will receive 50% off on all their clothes. Would you consider changing anything regarding your location information setting?

In the final and third part, the experimenter carried out another interview, this time with a semi-structured format, focusing on the users' experience, their impression of the proposed controls, and their perception about adjusting location privacy through the proposed controls. Except for the initial consent form, all other exchanges were done orally. Beside the participant, the only one present during the study was the experimenter who carried out the interviews, provided verbal instructions and took notes during the sessions. The same experimenter carried out all the sessions.

3.5 Results

We gathered data via the audio recordings and the notes taken by the experimenter. We transcribed the audio recordings from the study sessions, including both interviews and the interactions with the prototype. Afterwards, we coded and clustered the data based on the emerging themes. Our results provide some initial insights

regarding the usefulness of the proposed controls for location privacy management and also reports the users' preferences about location privacy adjustment through those controls. We also extracted numerical values from the choices participants made in each scenario and used this data to identify how participants' preferences changed between the two scenarios in each location. We then created transition diagrams based on these values. Finally, we carried out a chi-squared test to find out whether the proportions of the participants that chose a specific option in each of the scenarios differed between various locations.

3.5.1 Participants' prior experiences and perceptions of location privacy

During the initial interview, after being asked about prior experiences about location sharing, 20 out of 23 participants reported having never experienced any unpleasant incident because of sharing location data, while three had some unwanted disclosure of their location information. For example, P10 said: "*Yes, I wanted to surprise my wife, but she knew my location . . . we are sharing our location between each other, so she knew that I was in the shop; when I gave her the gift it was not a surprise anymore. From that time, sometimes I switch it off*". P14 and P18 mentioned experiencing a mild social awkwardness in different scenarios where both had tried to hide their location from a group of friends, but they were not successful. P19, on the other hand, said that he perceived the breach of his location privacy as a positive thing: "*Yes, but not bad but one very good one if you want to know. So there is also a Facebook app which normally wants to have access to your location, they look for when you got hacked, there was one person who tried to get into my account from another country, they sent me an email if it's me to check with me*."

We also asked participants about their current strategies regarding the protection of their location privacy. Only a few (5 out of 23) participants actively changed their location privacy settings, two turned off/on their GPS to save battery, and five only made such changes once (i.e. two navigation apps - two communication apps and one dating app). Eight participants claimed that they were not aware of any possibility of adjusting their location privacy setting, while two did not experience any lack of options for adjusting location privacy (P15 said that: "*there was always an option to change the default setting*" *and P19 thought turning off the GPS is enough*"); the rest did not feel the need to have such controls. Finally, participants were also asked if they think it is important to make any change to, or have control over sharing their location data: 12 said yes while five thought it was not that important; the rest were unsure.

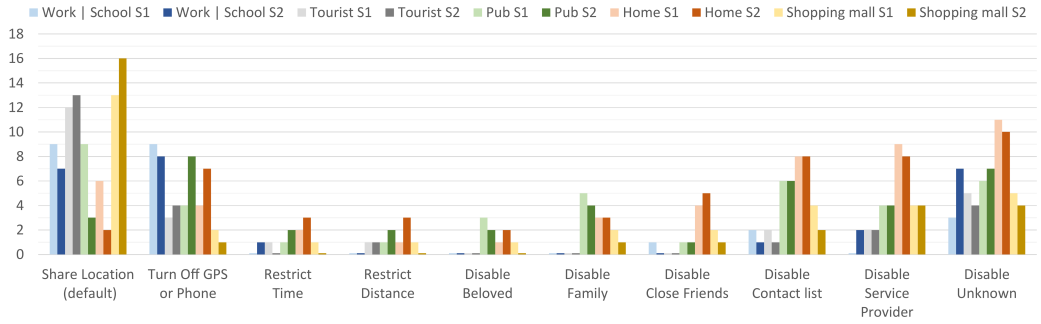


Fig. 3.6: Participants' privacy preferences in five different places: S1 refers to the base scenario, S2 to the notification scenario. Numbers correspond to how many people made use of a particular option to control their location-sharing settings.

3.5.2 Location sharing in different scenarios and places

Figure 3.6 summarises whom participants decided not to share their location with in the base and notification scenario, broken down by the different places used in the study. Since the default setting was assumed to be sharing with all groups, not taking any action meant keeping that setting activated.

As Figure 3.6 shows, N=6 participants left their location sharing activated at home in the base scenario. The majority of participants stopped sharing their location with service providers and unknown companies. This figure also reveals that almost half of the participants (N=12) were keen on sharing their location when visiting a new city in both scenarios. A similar pattern was observed in the shopping mall, where almost half of the participants (N=12) selected to share their location. This number increased to 16 participants after receiving the notification in the shopping mall notification scenario. At work or school, in the base scenario N=9 participants kept the default option and continued sharing their location.

A final observation from Figure 3.6 is that location sharing depends on the place and type of threat provided to the user. The histograms about sharing location (default) show that fewer people intended to share their locations when a threat was present in home/work/pub scenarios, whereas more people did share their location despite a threat in the tourist/shopping scenarios. This may have to do with the type of rewards obtained after sharing one's location. Work and Pub seem to not be the places where people want to be reminded about how they could improve their health habits. Fewer participants continued to share their location at home after receiving an invitation for dating. A suggestion of a good restaurant to a tourist, and discount possibilities to a visitor of a shopping mall increased the number of participants who were ready to give away their location information.

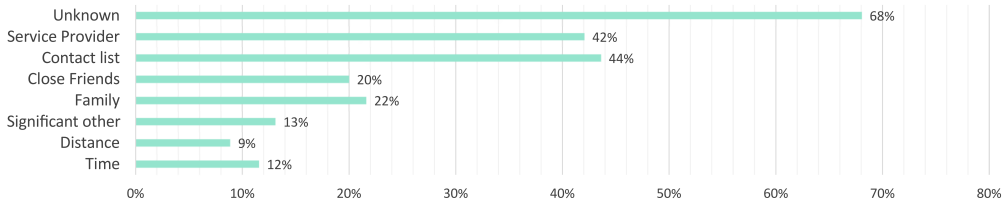


Fig. 3.7: Relevance of UI controls for location privacy management across all places and scenarios (average use in percentages of participants who used the interface; multiple controls could be used in a single scenario).

3.5.3 Relevance of UI controls for location privacy management

Figure 3.7 summarises how often participants who used the interface made use, on average, of the UI elements across all places and scenarios. In both of the two scenarios, participants could use multiple controls. From the mentioned figure, we can determine that the controls for specifying *whom to share with* were more popular than the time-/space-based restrictions. In this figure, it is also clear that the most used control was the one for toggling access for unknown companies, followed by those for the service provider and people on the contact list. Controls for close friends and family were used less frequently. The least-used controls were those facilitating the specification of time- or space-based restrictions.

Figure 3.7 also shows that the controls always seem to be applicable for location sharing at home, and in a pub (*all controls were consistently used in these scenarios*). This was less so for other places (i.e. new city, shopping mall and work/school scenario). In addition, none of the controls were never used, and this means that they are indeed relevant to location sharing (although perhaps to a different extent).

3.5.4 Users' expectations

Through the interviews after participants had used the interface prototype in the five places, we were able to gather some qualitative data about what users expect regarding location-sharing platforms. One of the observations relates to the default behaviour of such systems. Participants voiced a *preference for having location sharing turned off by default*. This result is in line with Patil et al. (2012), who observed that users preferred sharing location only upon explicit action. For instance, P13 said: "*I usually think by default the location is recorded, but it should be the other way around so I decide to share it now, and not because I forgot to turn it off*". And P2 echoes: "*There should be an option that does not ask me for how long I want to turn it off but for how long I want to turn it on*".

The following three quotes explicitly relate to the time control, but illustrate a similar idea: *"I really would like to say to Google, I just want to share my location for 10 minutes, because that's the time in which I'm going to arrive to this place, and after that I don't want to share it*" (P11); or, "*So, I would use the time in another way, so I turn it on, and use it as long as I need to and then it will automatically turn off*" (P15).

Some participants also explicitly mentioned their *wish to gain control over the accuracy of the location information that they share*. P22 stated: "*I would like to have one more option for giving a fake location or something like that*". And P23: "*I don't want anyone to know my exact location, so the city is ok but not my home address*". In addition to these two main expectations we identified, three participants also mentioned that is important for the UI to have easy access to its settings, as well as to have low effort levels for interaction (e.g. no typing). Other wishes include: sharing location with *everyone* in case of emergency (one participant), having a privacy manager that configures privacy options of all the applications which need location information (two participants), and being notified that someone is getting access to a user's location information (one participant). The variety of user expectations supports the idea of defining a set of *location privacy profiles* in a similar way to privacy profiles identified in Lin2014.

3.5.5 Feedback on the proposed UI design

Several participants gave positive feedback after interacting with the features provided by the UI we designed. P16, for example, stated: "*I think being selective with who you allow to know your location is the most powerful feature which this app is offering*". Some of the participants' comments gave hints about the possible reasons why the UI may have been well received:

- *Increased feeling of confidence and power:* This was a positive aspect highlighted by P10 and P18: "*I think in general it's really good to have more control because it makes people feel more confident*" (P10); "*They [i.e. the controls] are useful because all these location based applications I use [...] I feel like they should provide me some power, I don't want to reveal my information to everyone, this is almost the case whenever I use location-based services...*" (P18).

- *Increased control:* This aspect was emphasised by P3, P15, and P19. "*It's good to have extra options for restricting the location services, so in that way you feel safer and your privacy is controlled by you, whenever you want you can stop sharing with particular group of people ...*" (P3); "*I like this because it gives me the opportunity to change the data that is being sent everywhere and it also gives me the possibility of having control...*" (P19); and in P15's words: "*definitely the more control you have, the better it is...*".

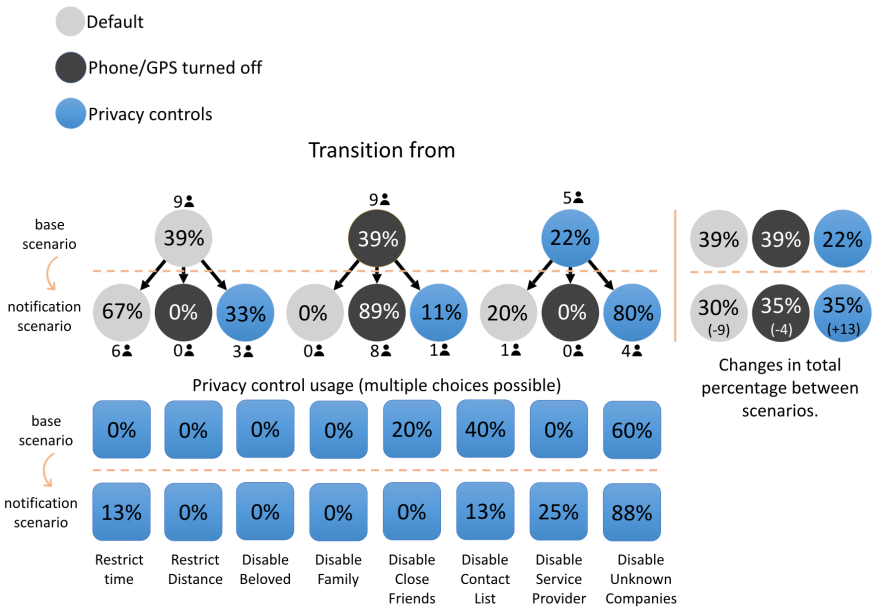
- *Having choices:* Some participants valued the simple fact of getting to choose. For example, P4 stated: "*it's important to have controls, at least a choice*"; P12 pointed out: "*I really like the controls because I don't only have the opportunity to restrict it to the persons, but also can restrict the time and distance*"; and in P13's view: "*it is very important that we have the possibility to decide whether to share information or not*".

In addition to these aspects, P10 also provided a positive review about the limited number of options provided by the developed UI: "*I think, it is definitely good to have such an option, it is also good to have some certain number of options, like three here, it's good*"; and P21 pointed at the possible usefulness of the controls to communicate with his family :"*I would use these controls to restrict my location for my family. So that will be useful for me*".

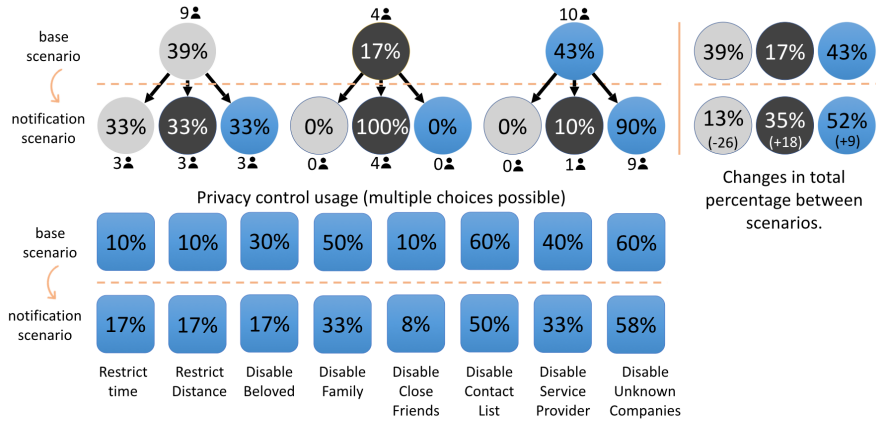
Furthermore, some participants also mentioned some aspects to consider such as the possibility that the new controls could generate an extra cognitive burden for the users which may not necessarily be worth the effort for them: "*It's interesting, but from my opinion, maybe it is kind of too much ...and I think this makes your life more complicated so always with these options and thinking of this stuff, I think it would be just better to think about other stuff instead of hiding your location...*" (P7).

3.5.6 Transitioning from base scenario to notification scenario

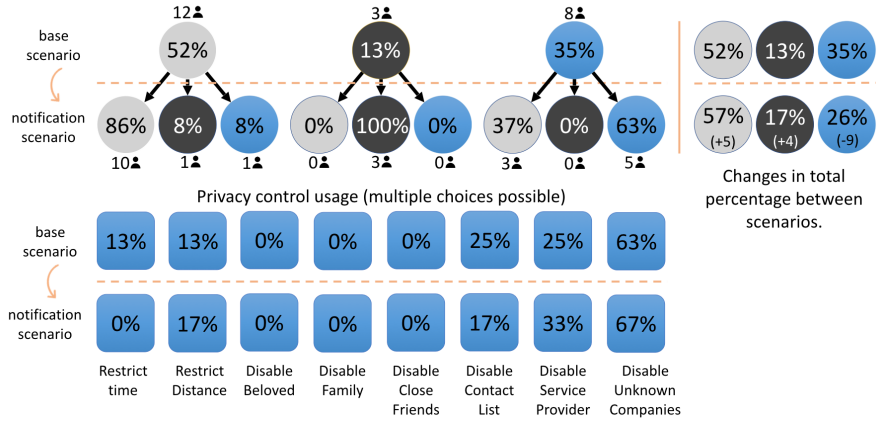
We also explored how control adjustment changed when participants transitioned from the base scenario to the notification scenario, i.e. which option they chose regarding their location information. We specifically wanted to find out if receiving an unexpected notification (i.e. a potential threat to their location privacy) had any influence on their choices regarding location privacy settings. We recorded each participant's choice/s in the base scenario and then observed their choices in the notification scenario. Figure 3.8 shows that the responses to the transition differed in different places and scenarios. In addition to learning about these differences, Figure 3.8 also presents in detail which privacy controls users picked (blue squares for both base and notification scenarios). In addition, the right top corner of the figure 3.8 shows for each scenario a general overview and changes on the total percentages among three groups (i.e. Default, Phone or GPS turned off and, Privacy controls). Numbers out of the circles on figure 3.8 represent the actual number of participants.



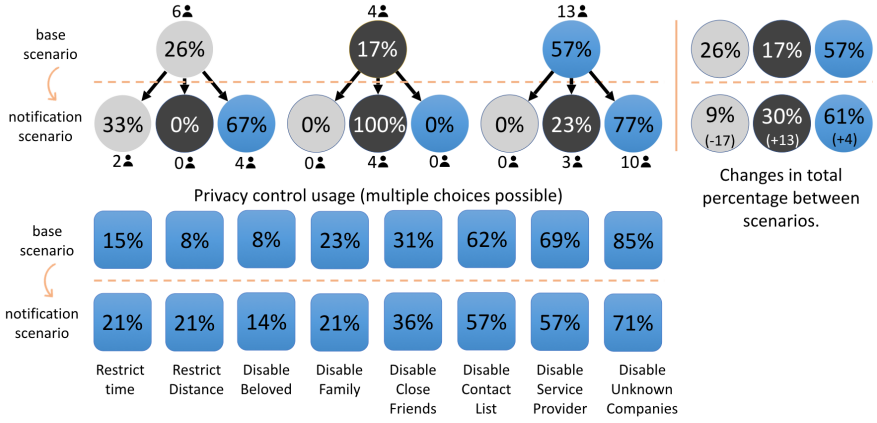
a)Transition diagram of users' location sharing preferences and privacy choices for the ***Work|School*** scenario.



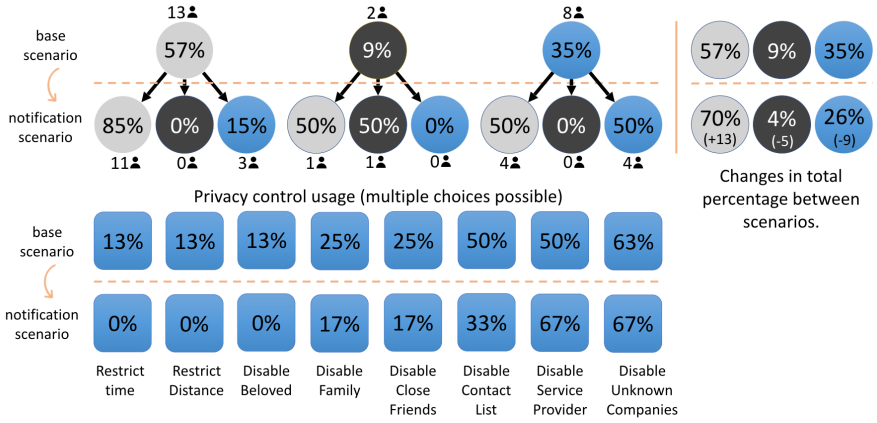
b)Transition diagram of users' location sharing preferences for the ***Pub*** scenario.



c)Transition diagram of users' location sharing preferences for the ***New city*** scenario.



d)Transition diagram of users' location sharing preferences for the ***Home*** scenario.



e)Transition diagram of users' location sharing preferences for the ***Shopping mall*** scenario.

Fig. 3.8: Transition diagrams of users' location sharing preferences for five scenarios.

In the *home* base scenario, 26% of participants were keen to share their location information (Figure 3.8d). However, after receiving the notification (i.e. someone close to your home wants to meet you), only 67% of these participants used some of the controls to restrict location information sharing, while 33% of them kept the same choice of sharing their location. Furthermore, among all participants who had used controls to restrict their location sharing in the base scenario at home (i.e. 57% of all participants), 77% decided to keep the controls option, and 23% turned their GPS or phone off in the notification scenario. We observed a similar trend towards further restricting location sharing upon receiving a notification for the 'pub/bar' location (Figure 3.8b).

In the case of the *shopping mall* scenario (Figure 3.8e), we observed a trend towards increased location sharing. The notification participants received here announced a 50% off sale from their favourite store in exchange for providing their location information to all retailers in the shopping mall. This apparently enticed most participants to freely share their location information, regardless of their choices in the base case. Somewhat countering this trend, amongst those who had let the default settings active for the base scenario (56%), 23% decided to use the UI to configure their sharing settings. A further trend that emerged is that in general, people tended to exhibit a similar decision in both scenarios. This was perhaps most pronounced for those participants who had decided to turn off their GPS/phone: in four out of five places, there were no changes at all when transitioning to the notification scenario. The only exception was the shopping mall, which seems to indicate that even 'privacy conservatives' can be enticed to share location given large enough benefits.

3.5.7 User preferences and places

Aside from the transition data, we wanted to test if the proportions of the sample population who went for different options in each location under the same scenario were different; i.e. we wanted to test if location and option were independent of each other for each scenario. We decided to group thematically related controls for the analysis, and this led to three clusters, namely time, distance, and social. The two controls to specify temporal and spatial constraints refer to the time and distance categories, respectively. The other six controls (i.e. significant other, family, close friends, contact list, service provider, unknown companies) were clustered as social. With that, we were able to separate the participants into three groups for each location and scenario: those who went for the default option, those who turned their phone or GPS off, and those who went for the detailed controls. A Chi-squared test was calculated comparing the frequency of how many participants chose each option in each location for each scenario. Our null hypothesis was that there is no relationship between location and the number of participants that go for each

option in a given scenario. Hence, our alternative hypothesis stated that there is a relationship between location and the number of participants that go for each option in a given scenario. At a significance level of 0.05, we could not find a significant relationship, χ^2 (8, N = 23) = 13.7338, p = 0.089, between the frequency of a chosen option and the location in the base scenario. In the notification scenario, however, we found a significant relationship χ^2 (8, N = 23) = 30.5018, $p < 0.001$ between the frequency of a chosen option and the location.

3.6 Discussion

In the following, we first reflect on the results we obtained in terms of how to interpret them and what implications follow from them. We then discuss limitations that the study and thus the results are subject to.

3.6.1 Usability of the location privacy controls

Overall, our results indicate that the proposed UI design for fine-grained control of location privacy settings was received positively by participants. This positive feedback provides some initial evidence that the theoretical model we used to create the UI may be useful to design user interfaces for location privacy with the potential of fulfilling users' expectations. By proposing three different layers for creating UI controls (i.e. privacy theory, privacy by design, user interface principles), the model provides means to approach the complex notion of location privacy in a systematic way. We found that all UI elements from Figure 3.2 were used during the study, but that the degree of usage varied considerably. Participants were most keen to control whom they share with, in particular whether they share with unknown companies. Considering that selling users' location information to third parties is an important business model of many 'free-to-use' location-based apps, this finding highlights a conflict of interest between service providers and their users. Another finding was that in contrast to the social restriction, the time- and space-based sharing restrictions were used rather rarely. On some level, this is somewhat surprising, given that previous work has found that people have strong opinions about which locations they want to (not) share (Tsai, P. Kelley, et al., 2009). It is possible that the underlying principle of using relative distance rather than named locations made the space-restricting option less attractive or less accessible to participants. With respect to the time-based restrictions, we hypothesise that the description of the scenario was devoid of temporal information (e.g. at what time of day and for how long participants were visiting these places) and thus did not easily facilitate the use of this option. This aspect could be investigated in more detail in a follow-up study.

3.6.2 Scope and relevance of the UI controls

Previous work (e.g. Consolvo et al. (2005) and Xie et al. (2014)) has indicated that *who to share location with* is an important factor of location-sharing behaviour. However, providing controls to assist users in sharing with different types of people has been underexplored. One of the few exceptions is the study by Assad et al. (2007), where the authors provided an early interface to control location sharing. The interface was web-based, and their goal was to enable people to choose how location information is revealed to other users of the MyPlace Locator system. The goal of the present work is a bit different, in that the scope is not limited to a specific system. Instead, our aim was to contribute to a broader understanding of useful controls for location sharing by mobile phone users. Accordingly, the insights garnered here have a broader scope. In particular, the positive feedback obtained from the participants suggests that the implementation of the controls from Figure 3.2 (or some of them) is likely to have a positive impact on location privacy management in current mobile phones.

The relevance of the proposed UI based on social, temporal and spatial adjustments were also presented in our results. Early studies such as Scipioni and Langheinrich (2011) and Stroeken et al. (2015) have pointed out the importance of such factors in protecting location privacy. Our approach is different in that 1) we gathered three factors and 2) presented them as an accessible UI at the Operating System level. We suggest that such a UI that facilitates the adjustment of location-sharing settings should be available for users and for every application that exploits users' location information.

3.6.3 User preferences

Xie et al. (2014) identified users' location sharing preferences based on a number of hypothetical scenarios. Their study included seven different types of people (i.e. single, family, kids, spouse, girlfriend, friends, colleagues). The study in this work is similar in that it also collected some location-sharing preferences based on hypothetical scenarios. There are some overlaps in terms of the types of people considered (e.g. family, significant other, and close friends appear on both lists). Furthermore, the work included *advertisers* from (Benisch et al., 2011; J. Lin, Benisch, et al., 2013) (covered via the control for service providers). Since there is a variety of people and/or institutions that one could share location information with, future work will benefit from a typology of requesters of location information. In addition, Xie et al. (2014) found location- sharing preferences to be context sensitive and audience aware. Figure 3.7 shows some observations along the same lines: one can see that the preferences of the participants are context sensitive (i.e. they depend on the type of place), but are also audience aware (i.e. they vary according to who).

However, the fact that some participants did not react as expected (e.g. participants stopped sharing their location when given “useful" tips at work about their health) suggests that location privacy preferences may also be *incentive aware*.

In all scenarios, we intended to design a positive notification as an indicator for the invasion of location privacy, but participants perceived these threats differently. In the New city and Shopping mall scenarios, they valued the information they received higher than the risks of letting everyone know where they are. This observation also shows that due to the complex notion of privacy and digital privacy specifically, there *might be different perspectives on how the designers of a service value privacy and how end users might perceive it*. Ward et al. (2005)’s study shows that the participants in their study had concerns about providing financial information but saw no problem about providing personally identifiable information. This highlights, once again, that users need to be made aware of the importance of location privacy in general, it also shows the importance of addressing privacy-related issues before or during the design of the services since factors such as different perspectives on values, or various perceptions on incentives might lead to challenges regarding the acceptance and use of the service by end users. One way to address such challenges could be including users in the process of developing a service and ask them directly about their values regarding their location information and the services they can receive while making sure they understand the threats associated with sharing location information.

3.6.4 Configuring location privacy settings

It is important to highlight the underlying trade-offs of configuring location privacy settings. On the one hand, the fine-grained controls we provided enabled participants to specify in detail how and with whom they wanted to share location information. They were also able to respond to potential privacy threats in a nuanced way. On the other hand, managing location privacy is certainly more complex than a simple ‘on/off’ switch via UI controls. It also seems that given the right incentives, people give up their location privacy willingly. Regarding UI and privacy management, Cranor et al. (2006) stated: *user interface designers need to find ways to manage the complexity, educate users about privacy, or express privacy concepts using language they already understand, guide users through the process of expressing their privacy preferences, and offer various options that meet the needs of a diverse set of users*. There are thus many parameters at play, and even if the proposed UI was well received, the results highlight the need for more studies to look further into aspects - if any - of context, audience, and incentive which make location sharing predictable.

Besides, as mentioned in Section 3.3.2, the UI supports at the moment six types of stakeholders: family, close friends, the user’s significant other, user’s list of (known) contacts, app and service providers, and third parties unknown to the users but which

might potentially get access to her location data. It is acknowledged here that these six stakeholders are not mutually exclusive when it comes to sharing location data (e.g. current location-based services necessitate a service provider, a family member may also be a close friend at the same time). However, the fact that many users in the scenarios precisely wished not to share their location with some stakeholders while sharing it with some others (see Figure 3.8) calls for *fine-grained location management at the technical level*. For instance, future generation location-based services - if they are to be more user-friendly and privacy-aware - should provide technical means for users to share their location with peers without service providers knowing. If sharing location to peers without involving service providers turns out to be impossible or impractical, ephemeral location-based services (Ataei and Kray, 2017) could provide a good alternative (i.e. service providers could still act as brokers between two users interested in exchanging their location information but automatically delete users' records when the receiver got the information provided by the sender).

3.6.5 Limitations

Our study was subject to some limitations which also restrict the generalisation of our results and the conclusions we drew from it. First, despite our efforts to simulate the conditions of the five previously described places (through the use of panoramic pictures in the IVE (Delikostidis et al., 2015)), the participants for the home or work locations did not see pictures of their actual places. To address this, we asked them to imagine being in their owned places, but there is the possibility that the participants might never actually have perceived receiving unexpected notifications as a threat in a place where they expect privacy. Also, they did not use their own mobile phones but the one we provided for them. Since we also conducted the study in the lab (rather than in the real world), the ecological validity of our study is limited.

Second, during the initial part of the study, we asked questions about their general opinions regarding location privacy. This might have influenced their use of the developed prototype, as they were aware that the study was about location privacy (e.g. they might have pretended to be more concerned than they are on a regular basis). Furthermore, we asked participants to think aloud and report their actions, which could have impacted their choices as well. A closer look at Section 3.5.1 and the answers provided by the participants during the first interview suggests that most of the users were not highly concerned (i.e. rather unconcerned or "fence-sitters" in J. Lin, Liu, et al. (2014)'s typology). Further work is needed to investigate the sensitivity of the results obtained with respect to variations in the types of profiles of the participants. Third, further limitations result from the relatively limited number of participants and the resulting small sample size for

statistical analysis. Since our primary interest was to obtain rich, qualitative data we had to make this trade-off to keep the effort of realising the study manageable. We also only presented a small number of scenarios to users based on other studies reported in the literature. In real life, people visit many different locations that we did not include in our study, and these other places could trigger more sensitivity regarding location privacy.

Finally, Figure 3.1 pointed that out that few features of the model (e.g. error handling, end-to-end security, full functionality) still need to be implemented for the proposed UI. Though omitting these features is likely to have had an influence on the results presented in this work, the exact nature of this influence would need to be investigated in future work (e.g. through new iterations replicating the current study).

3.7 Conclusions

Overall, we presented a method for designing user interfaces (UIs) for location-based services. We used this method to design a prototype that provides controls to users for managing location privacy. Moreover, we implemented and evaluated the privacy control prototype through an empirical user study to assess the usefulness of the controls for adjusting location privacy. Our results show that in the majority of locations, about 35% (median) of the participants chose the provided controls instead of default sharing settings regardless of the scenarios. The results also shows that from the participants who selected the provided controls, the social controls were the most frequently used (median $\bar{7}8\%$). These particular controls were designed based on Westin's privacy theory.

In general, location privacy is an important issue which should be addressed by developers of location-based services if they are hoping to build services that are going to comply with current and future location privacy protection regulations and that are going to be accepted by users who have location privacy concerns. UIs can play a significant role in conveying to users the importance of location information protection. UIs can also increase transparency regarding what is being shared with whom, when and where, such factors are crucial to address while designing privacy protected services. This option of providing controls through UIs to users will lead to an increased trust and better acceptance of technology, which can also represent a gain also for service providers and developers.

Based on our research, there is a strong need for further work that supports developers in building location-based services that are also location-privacy aware. In addition, research is needed regarding how to make users aware of threats and control mechanisms regarding their location privacy. Longitudinal studies with the proposed UI controls would also benefit the overall understanding of user behaviour and preferences with respect to location privacy. Finally, the development of privacy-aware LBS can benefit from further studies on the use and evaluation of the proposed model by developers and designers of LBS.

4

Complying with Privacy Legislation: From legal Text to Implementation of Privacy-Aware Location Based Services

> *The good of the people shall be the supreme law.*
>
> — **Marcus Tullius Cicero**
> (The De Legibus)

This chapter was submitted in preparation for the journal of GEO-information as Ataei M., Degbelo A., Kray C., Santos V. (2018) "Complying with Privacy Legislation: From legal Text to Implementation of Privacy-Aware Location Based Services.

The location data of individuals is very sensitive geoinformation. While its disclosure is necessary, e.g. to provide location-based services (LBS), it also facilitates deep insights into the lives of LBS users as well as various attacks. Location privacy threats can be mitigated through privacy regulations such as the General Data Protection Regulation (GDPR), which came into force recently and harmonises data privacy laws across Europe. While the GDPR is meant to protect users' privacy, it does not provide explicit guidelines for designers and developers about how to build systems that comply with it. In order to bridge this gap, we systematically analysed the legal text, carried out expert interviews, and ran a nine weeks long take-home study with four developers. We particularly focused on user-facing issues as these have received little attention compared to the technical issues. Our main contributions are a list of aspects from the legal text of the GDPR that can be tackled at the user interface level and a set of guidelines for how to realise this. These guidelines were evaluated in a take-home study. Our results can help designers and developers of applications dealing with location information from human users to comply with the GDPR.

4.1 Introduction

Many services routinely collect location data from human users for various reasons. While there are many benefits of the availability of personal location data (e.g. better

personalisation, location-based services), this type of geoinformation is particularly sensitive as it allows for deep inferences about the person who produced it. For example, location data can be used to find out where individuals live, whom they interact with and what their daily routine is (Krumm, 2009). In addition, even very few data points can be exploited for attacks such as stalking or breaking into someones home while they are away (Clarke and Wigan, 2011). Recently disclosed privacy violations have led to further increasing worries regarding surveillance (Y.-W. Lin, 2018);michael2011social. It thus makes sense that technical as well as legal measures are being developed to ensure the safety of service users as well as their basic civil rights and freedoms.

The General Data Protection Regulation (GDPR) (EU, 2016) is such a legal safeguard that harmonises data privacy laws across Europe. It was introduced by the European Parliament and the Council of the European Union (EU), to strengthen the protection of people with respect to the processing of their personal data. The GDPR was first published in April 2016 and fully applied since May 25, 2018, onwards. It includes far-reaching measures to protect privacy and is widely expected to be a game changer for the design of computing systems in general – including those that specifically function based on location data of their users, i.e. location-based services (LBS). Given that in the digital age "privacy goes global" (Newman, 2015), the impacts of GDPR will be felt far beyond the boundaries of Europe.

While this new law promises to strengthen the rights of individuals, it is also poses challenges to the designers and developers of systems that process personal data (e.g. location data). On the legal level, there are questions such as how compliance can be demonstrated. On a technical level, the law introduces new requirements regarding how data is stored, processed and deleted. While these two perspectives already introduce many challenges, it also not clear how to realise various requirements that the GDPR formulates with respect to what users should be able to control and regarding how and when certain types of information should be presented to them.

Location-based services (LBS) are an increasingly ubiquitous type of systems that deal with geo-information and process location data of their users. In this paper, we aim to address challenges resulting from the introduction of the GDPR that relate to the user interface of LBS. Our main contributions are as follows: (1) We systematically analysed the legal text to identify a list of aspects that can be tackled at the user interface level (UI) (Section 4.3); (2) In addition, we carried out interviews with experts to gain further insights into challenges arising from having to comply with the GDPR as well as into ways how and when to address them (Section 4.4); (3) Based on the outcome of both activities, we compiled a set of guidelines for developers and designers to help them to design LBS that comply with the GDPR (Section 4.5). Finally, these guidelines were evaluated in a take-home study with four developers. The participants developed two fully functioning LBS prototypes while using the guidelines (Section 4.6). Our contributions can benefit

designers and developers who need to create services that meet the location data related requirements defined by the GDPR.

4.2 Related work

In this section, we briefly summarise key related work by first reviewing various concepts and definitions of privacy and location privacy. We then provide a short overview over the GDPR – an in-depth analysis of the legislation is subject of the subsequent chapter – and outline how location data privacy and LBS are connected. This is followed by a brief review of existing approaches to tackle location privacy issues in LBS. A summary concludes the section.

4.2.1 location privacy: definitions and concepts

Although there is no single and simple definition for privacy, it is important to gain an understanding of the facets that define and shape it in order to build privacy-aware technologies. According to Westin (2003), privacy is "*the claim of an individual to determine what information about himself or herself should be known to others.*" *In addition, it also makes a difference how such information is obtained by others and what it is then used for*". Westin (2003) further defines three levels on which privacy issues can be addressed: at the political level, the socio-cultural level and the individual level. Obviously, different political systems and philosophies will vary with respect to how much value they attribute to individual freedom from surveillance versus maintaining public order. Legal frameworks, such as the GDPR, are the means by which these different values can be expressed. Privacy at the socio-cultural level relates to individuals' practice and experience in their everyday life, or as Westin puts it: "*the real opportunities people have to claim freedom from the observation of others ...*". In this sense, privacy is frequently determined by the individual's power and social status Westin (2003). At the individual level, Westin (2003) distinguishes four basic states: solitude, intimacy, anonymity and reserve. Solitude refers to the right to not being observed by other parties. Intimacy covers the right to entertain a close, honest and relaxed relationship with one or more people (a small group). Anonymity refers to being free from surveillance in public, and reserve denotes the right to limit what information about oneself is disclosed to other parties.

While privacy thus is an important and complex concept in our everyday lives, this is especially true in the context of our digital endeavours. D. Solove (2008) confirms this by stating that: "*privacy is a plurality of different things and that the quest for a singular essence of privacy leads to a dead end*". Conceptualising privacy can be achieved by discussing six general heading, which include: "*(1) the right to be*

let alone; (2) limited access to the self, the ability to shield oneself from unwanted access by others; (3) secrecy, the concealment of certain matters from others; (4) control over personal information, the ability to exercise control over information about oneself; (5) personhood, the protection of one's personality, individuality, and dignity; and (6) intimacy, control over, or limited access to, one's intimate relationships or aspects of life. Some of the conceptions concentrate on means to achieve privacy; others focus on the ends or goals of privacy" (D. J. Solove, 2002).

The importance of data privacy becomes more clear when a specific kind of data can pose a substantial risk to individuals' safety and privacy, sometimes without even their knowledge. Information about individual's location is one of those kinds of data which has a great potential to identify users personally but also if combined with other types of data such as finance or health can reveal sensitive information about individuals.

Location data is being used in the majority of the services that provide users with relevant information to their geographical positions (i.e., LBS). The presence of "*ubiquitous positioning devices and easy-to-use APIs make information about an individuals' location much easier to capture than other kinds personally identifiable information*"(Keßler and McKenzie, 2018). Protection of location data is important due to the increasing number of technologies that collect, process and store location data of users and the sensitivity of such data as if it disclose can reveal confidential information about individuals and eventually pose risks on the individual's life. Even if users do not explicitly share their geographic coordinates, their location can be probabilistically determined based on the words that they write (e.g. on Twitter), the timestamps that they make public, and a basic understanding of the spatial properties of a city (see McKenzie et al., 2016). In general (and as indicated in Fawaz, Feng, et al., 2015), a location privacy threat is a function of the current location along with previously released locations.

As LBS function based on location data, in order to address potential privacy-related issues, it is crucial to understand and define location privacy in this context, then explore possible threats associated with it and finally implement countermeasures to mitigate such threats. Duckham and Kulik (2006) define location privacy as "*a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others*". In order to design a GDPR-compliance UI for LBS, the first step is to understand LBS, location privacy, and the importance of protecting personally identifiable information (PII) including location data.

4.2.2 location data privacy issues in LBS and the role of the General Data Protection Regulation (GDPR)

Personally identifiable information (PII) that includes location data is one of the key factors relating to privacy in the digital realm. This refers to any information that can be linked back to a natural person and therefore provides a third party with a potential vector of attack. For example, knowing a person's current location might enable a third party to threaten or expose that person. Since such information is very sensitive and potentially dangerous in the wrong hands, laws are put in place to protect it and regulate its use. In the European Union, the European Commission has issued the General Data Protection Regulation (GDPR) EU, 2016, which is an expanded and harmonised version of Directive 95/46/EC (Data Protection Directive or DPD). It defines far-reaching rights for individuals with respect to PII that relates to them. It applies to any company, which processes or collects personally identifiable information of an individual in the E.U., e.g. in the context of providing services or selling products. This includes companies based outside of the E.U. if they process or collect such data. Companies that do not comply with the GDPR face hefty penalties. The many requirements set out by the GDPR are predominately focused on the way companies handle PII, which in some cases may require substantial changes in order to become GDPR-compliant. While some of these changes will affect 'behind-the-scenes' data management, other aspects will require direct user interaction, i.e. changes at the UI level. A detailed analysis of the latter is the topic of section 4.3.

The previous paragraphs already illustrate that privacy is an important issue to consider in designing services: not only are they routinely collect personally identifiable information, but they also process it in different ways. The GDPR has a very broad definition of 'processing information', which includes "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*"(EU, 2016). Consequently, almost any system that allows users to register or personalise its appearance or functioning would fall under the GDPR. For example, personalisation of a web application can affect links that users see when they interact with the system, the content that they are presented with, and the overall structure of the web application (see (Danculovic et al., 2001)). In earlier work, Kobsa (2007), providing an introduction to the field of privacy-enhanced personalisation, pointed out that online users value .personalisation. At the same time, personalisation of Web sites seems profitable for Web vendors. Automatic content customisation creates, therefore, a win-win situation for both. Nevertheless, since users need to give up some data in exchange for tailored content, there is always a

privacy threat associated with personalisation on the Web. Kobsa (2007) brought forth two factors which impact the type of data being collected, and the methods employed for processing the data in the context of privacy-enhanced personalisation. These are user concerns and privacy regulations.

Another example, where LBS process PII, is the use of location-information to adopt a service to where the user is located (aka location-based services). This does not only include classical navigation systems but increasingly is used to adapt web pages, apps and advertisements. Location information is particularly sensitive information as it allows deep inferences about the person being tracked (Beresford and Stajano, 2003) while at the same time also being very useful to detect the context of a user and to adapt system behaviour. Location adaptation and personalisation are only two of many examples where LBS process personally identifiable information, and can thus cause privacy issues. While a number of research studies location privacy from various aspects such as technological, legal, ethical, or educational, Keßler and McKenzie (2018) in their "manifesto" on Geoprivacy (i.e. location privacy), argue that the complex matter of addressing location privacy must be considered as a whole, integrating all these involved aspects.

Location privacy issues in LBS can be tackled in different ways. A large body of work exists discussing various attacks as well as key concepts and technologies such as k-anonymity (Sweeney, 2002), mix zones (Beresford and Stajano, 2003) or the Casper system (Mohamed F Mokbel et al., 2006). Beyond approaches that focus on very specific aspects (such as location privacy), there are also some more general proposals about how to make LBS more privacy-aware. Langheinrich (2002) specifically looked at ubiquitous systems and proposed an approach to ensure accountability rather than guarantees regarding PII. His approach can also be classified as following many of the guidelines laid out by Privacy-by-Design (Cavoukian, 2009), which defines seven basic principles that interactive systems should realise to protect the privacy of users. While technical advancements are necessary for improving the protection of location privacy, Keßler and McKenzie (2018) state that "*Preserving geoprivacy involves more than obfuscating geographic co-ordinates. Location can be inferred from non-explicitly geospatial information such as interests, activities and socio-demographics*". One of the concerns in this regards is related to the mobile operating system that "*lack fine-grained control mechanisms for location services, thus severely limiting the degree of control users have over their location information*" (Keßler and McKenzie, 2018). Ataei, Degbelo, et al. (2018) have recently proposed user interface elements for fine-grained management of location privacy settings which helps to specify whom to share location with, when to share it, and where to share it.

While there is a number of critics aiming at legal countermeasures like "The ethical ramifications of advances in location-enabled technology are often viewed as an afterthought, and legal concerns over privacy aspects lag behind technological advances" (Keßler and McKenzie, 2018). GDPR has tried to overcome such critiques by integrating privacy by design principles such as privacy embedded into the design,

privacy as the default setting and also visibility and transparency regarding the data collection activities (Cavoukian, 2009). Addressing location-privacy related issues is a complex matter and needs clarification, discussion and proper actions. To keep this work feasible, we will focus on only a few aspects of this process. The location privacy in LBS will be a core area to focus on, in this context, we will study the implementation of Legal requirements, we categorised those requirements and will focus on those that are addressable through UI.

4.2.3 Summary

From this brief review of related work, we can draw a number of conclusions. While privacy is a complex concept, it plays an essential role in everyday life, and in particular, in the digital realm. Many services process PII such as location information for various reasons (e.g. service adaptation, personalisation, in-kind payments) and can thus cause different types of issues. One of the critical concerns regarding the default behaviour of such services is related to the presence of controls for location privacy settings (sharing all or nothing). In the majority of the cases, users are not provided with means to adjust the personal data collected about them through services. In addition, such services are subject to the corresponding legislation such as the General Data Protection Regulation (GDPR), which was recently put into law in the European Union. While various approaches have been proposed to tackle privacy issues in LBS, how exactly these could be used to make a system compliant with the GDPR is not clear. In the remainder of this paper, we will, therefore, look deeper into this issue.

4.3 Analysis of the GDPR

GDPR (EU, 2016) consists of 99 articles and 173 recitals, including principles such as conditions for law fullness processing, rights of the data subject, responsibility of controller and processor, to name but a few. Among many aspects presented in GDPR, there is an emphasis on transparency, providing controls for data subjects over their data and following the principle of privacy by design.

We explored various strategies for interpreting GDPR's text document from developers and designers perspectives. We eventually developed a strategy including six iterative steps with the goal of understanding the legal requirements and assigning them to the responsible individuals. The six steps involve: 1) scan: a thorough scanning of the legal content; 2)extract: extracting requirements; 3)clarify: clarifying the expectations of the legal text; 4) cluster: clustering them into categories; 5) relate: relate, connect or translate them into understandable terms for developers;

and 6) assign: assigning the requirements to responsible individuals.

With regard to these aspects, we compiled the most relevant set of provisions for designing LBS in GDPR, and categorised them into two groups: 1) *data management* which includes minimising data collection, secure storage and keeping the data accountable (i.e. updated and correct); and 2) *communication of data management with data subjects* that includes notifying data subjects about collected personal data, conditions for consent and providing controls such as access, rectification, and restriction based on the right of data subjects.

In the area of developing privacy-aware LBS, there has been more advancement on technical (i.e. back end) level than front end (i.e. presentation or UI) level. Therefore, to explore the latter and also keep the scope of this work manageable, we chose to focus on communication data management with users or front end with an emphasis on the requirements which are addressable through UI design, namely: Notice, Consent, and Control. We will discuss the legal requirements for each of these factors in next sections. These requirements have been derived from the GDPR content (EU, 2016). For the purpose of this paper (inferring concepts and principles), we are using the same terms and definitions that are presented in Art. 4 definitions of GDPR (EU, 2016). The following terms (and their respective definitions) are relevant in the context of this work:

- 'personal data' means any information relating to an identified or identifiable natural person. 'data subject', an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

- 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

- 'processing' means any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemi-

nation or otherwise making available, alignment or combination, restriction, erasure or destruction;

- 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

- 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

One of the GDPR's major concern is related to the data subject's rights. Compliance with GDPR requires understanding these rights and also building services with respect to these rights. GDPR requires service providers (i.e. data controllers and processors) to support transparent communication (Art.5). Respecting data subjects right and communicating the processing activities to data subjects are GDPR's requirements in this context. Our analysis of GDPR has focused on data subject's rights and the aspects that are addressable at UI level. This analysis resulted in three primary categories, Notice, Consent and Control. A short explanation for each of the factors is going to be presented in the following sections. A more detailed version of the analysis including all relevant Articles and Recitals from GDPR is included in Appendix 4.9.

4.3.1 Notice

GDPR requires the ensuring of lawful, fair and transparent processing of personal data. According to the recital 60 of GDPR (EU, 2016), the processing is fair and transparent if the data subject is informed of the existence of the processing and its purposes. The controller should provide data subjects with the information that is listed in Art. 13 of GDPR which includes, (a) the identity and the contact details of the controller; (b) the contact details of the data protection officer; (c) the purposes of the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients of the personal data. In addition to the list, data subjects should also be informed about: (a) the period for which their personal data will be stored; (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; (c) the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based

on consent before its withdrawal; ... (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject Art.13 - (EU, 2016).

Informing data subjects about their rights, the consequences of their decisions and the activities of the controller can ensure fairness and transparency regarding the lawfulness of the processing. GDPR considers the processing lawful if "*the data subject has given consent to the processing of his or her personal data for one or more specific purposes*" or processing is necessary for various reasons such as " *compliance with legal obligation*" or " *for the performance of a task carried out in the public interest*" Recital 60 -GDPR.

4.3.2 Consent

According to the GDPR, consent is one of the fundamental principles to make data processing activities lawful. Article 4, defines consent of data subjects as *any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her* (EU, 2016). Article 7. defines conditions for the consent such as (1) where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data and (2) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. Recital 42 also lists some requirements for consent: *for consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment*.

The consent should communicate the processing activities with data subjects which is similar to notice, but the primary difference is that the consent requires active approval and confirmation from data subjects. It also needs to be flexible to support the features of withdrawal (i.e. the right of opting out from data processing) and renewal (i.e. receiving an updated consent when the purpose of the processing has changed).

4.3.3 Control

GDPR stresses the importance of providing data subjects with control over their personal data. Control includes various principles such as the right of access, the right to rectification and erasure, the right to restriction, the right to data portability and the right to object. We will briefly explain the legal requirements for each.

- Access - according to Art. 15: *The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed* (see appendix 4.9 for the listed conditions according to Art.15).

- Rectification - Art. 16: *The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her*.

- Erasure ('right to be forgotten'): *The controller shall have the obligation to erase personal data without undue delay where one of the following grounds* listed in appendix 4.9 applies.

- Restriction of processing - Art. 18: *The data subject shall have the right to obtain from the controller restriction of processing where one of the following grounds* listed in appendix 4.9 applies.

- Data portability - Art. 19: *The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided Art 20*.

- Object - Art. 21: *The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1)*. See appendix 4.9 for the details.

Fig. 4.1: Word cloud of terms mentioned at least 200 times in the GDPR reference document (EU, 2016). It helps see most prominent concepts of the regulation: personal data, the processing of it, and the interaction between controllers and (data) subjects. The word cloud was generated in March 2018 using Wordart (`https://wordart.com/`; last accessed: March 26, 2018)).

4.3.4 Summary

The previous three sections have presented the provisions of GDPR with respect to data management, and communication of the data management to the data subject. As the reader may have noticed, the terms 'data subject' and 'controller' come over and over again. They stress the importance of both parties for the lawgiver. In fact, a word-cloud (see Figure 4.1) which displays words found at least 200 times in the GDPR reference document (EU, 2016) makes clear what GDPR is all about: it's primarily about personal data; the processing of it, and the *interaction* between controllers and (data) subjects. Note that 'interaction' is used here is in line with Hornbæk and Oulasvirta (2017) who argued that "interaction concerns two entities that determine each other's behaviour over time " (emphasis original). GDPR-compliant services are therefore mediums which support that mutual determination between the controller and the data subject. The regulation puts a clear emphasis on the role of controllers, but the processor (a bit less prominent on the figure) is also a third important actor. In fact, the processor was already identified by Conger et al. (2013) in their model of personal information privacy[1]. That is, in the digital age, GDPR-compliant services are systems which support the mutual determination

[1]There are some parallels between the roles listed above and the roles listed by Conger et al. (2013) in their model of personal information privacy. The 'individual' of Conger et al. (2013) is equivalent to the 'data subject' of GDPR; the 'vendor/providers of services' from Conger et al. (2013) are akin to 'controllers' of GDPR; the term 'processor' from GDPR includes both the 'third party' (i.e., data

between the controller (i.e. the entity which requests personal data), the data subject (i.e. the entity which gives personal data away), and the data processor (i.e. the entity which processes personal data). The next section points at some of the challenges (viewed through the lenses of experts) of implementing GDPR-compliant IS, and possible ways of addressing them.

4.4 Experts Interviews

A set of interviews was conducted to explore challenges and solutions regarding the implementation of GDPR. We started the process with a planning phase, with a few research questions, and we gathered reflections from experts in three main areas: general challenges, possible solutions, and specific requirements for Notice, Consent and Control (i.e. NCC factors). The specific requirements touched upon what to include in each NCC factor, how to communicate it to users and the phase of system development where they should be considered.

4.4.1 Participants

The participants were domain experts who were directly involved with implementing GDPR in an academic or industry environment. Besides GDPR involvement as the main requirement, experts were recruited based on their experience in the field of data privacy, data ethics and security in information systems. Six experts, two from industry, three from academia and one from both participated in our study. Detailed demographics can be found in the table 4.1.

4.4.2 Procedure

We conducted semi-structured interviews through video calls (via Skype). We found semi-structured interviews appropriate as our goal was to gather deep insights and receive critical comments about the topic. We divided the questions into three levels. Level one included the intro question (i.e. participants role and experience with data privacy or GDPR) which was followed by questions regarding the general aspects of the topic, including challenges regarding the implementation of GDPR and possible ways of addressing such challenges. Level two consisted of a more specific set of questions including some that targeted difficulties which developers and designers could encounter while developing interactive system regarding GDPR compliance.

sharing partners), and the fourth party (i.e., illegal hackers, thieves and third-party employees who violate company policy) from (Conger et al., 2013).

Level three was a focused inquiry on particular questions regarding NCC factors (i.e., Notice, Consent and, Control), including the phase of system development in which one should consider NCC factors, what to include in each phase and how to communicate the relevant information to end users at the UI level (see Figure 4.2 for details). The lead author carried out all the interviews, provided a verbal explanation, received digitally signed consent forms from participants and took notes during the sessions. All the sessions were audio recorded after participants had consented. The institutional ethics review board approved the study prior to its execution.

Participant ID	Brief Biography
E1	Professor and consultant working on design ethics
E2	E-Governance evangelist, currently part of an expert group advising a European city council on matters related to the implementation of GDPR in relation with government and public services
E3	Assistant professor working in projects related to data justice, and specials in data ethics.
E4	Lawyer, currently advises companies at the moment in different sectors like banking, insurance, transportation with respect to the implementation of GDPR
E5	Professor and co-Founder of an IOT (Internet of Things) company, which develops solutions for smart cities
E6	Professor, currently working closely with municipalities on the implementation of smart cities initiatives

Tab. 4.1: Brief biography of the experts interviewed.

4.4.3 Results

The analysis of data started by transcribing the audio recording and the notes were taken by the interviewer. We used directed content analysis to analyse the data. The directed content analysis involves the use of categories or codes defined by the researcher prior analysis and may lead to the definition of some further (sub)categories during the analysis (see (Hsieh and Shannon, 2005)). We used MAXQDA 2018 as a tool to code and analyse the data. The codes were specified at the beginning of the analysis based on the questions that we asked: 1) Challenges regarding the implementation of GDPR (i.e. including particular difficulties for developers and designers in the context of GDPR implementation); 2) Suggested solutions by the experts to tackle the challenges; 3) When (during interactive system development) to address GDPR and who is responsible for the GDPR implementation; and 4) Specific recommendations from the experts for the implementation of Notice, Consent and Control at the UI level. The answers that emerged from each category are reported in the following sections. Since it is well known that experts often disagree among themselves, a (sub)category related to one of the codes defined

above was created only if at least two different people referred to the topic of the category.

Challenges regarding the implementation of GDPR

The following challenges and how to address them were mentioned by the participating experts:

User-friendliness: not surprisingly, implementing GDPR in a way that does not place some unmanageable burden on users was mentioned by the participants as an issue. Implementing GDPR while avoiding complexity in interaction or overwhelming numbers of alerts or notifications was mentioned by E1 and E6. Also, the importance of communicating privacy-related issues to end users in a simple way was mentioned by E1, E2 and E5.

Awareness: Raising awareness about the necessity to think early during application development about data protection was also mentioned as an important challenge. E4 believed that start-ups and some business do not have enough resources to consider privacy-related issues from the beginning stages of system development.

Technical considerations: Technically realising the requirements of the regulations is a further challenge. Guaranteeing anonymisation is difficult due to the currently available technology options according to E5 and E6.

Regarding specific challenges for developers and designers, participants highlighted the following problems, namely:

Lack of specific guidelines: E5 who is a founder of company developing IoT devices said: " *in my company, we have developers and we are trying to develop software solutions, and we have not found any guidelines that we can use'*. A similar concern was raised by all other participants.

Reasons for compliance with GDPR: This was another challenge, mentioned from different perspectives. Participants also raised concerns about the need for proper education regarding the importance of compliance with GDPR (similar statements by E1, E3 and E5). E1, for example, stated that *'designers need to be told clearly in the brief about the compliance with GDPR,..., designers ought to know the purpose of compliance, designers should know the context and reasons'*. E3 also said that *'we could explain to designers what kind of value they think they should include or how to include those values'* to comply with GDPR. The overall difficulty was to find a way to provide developers and designers with explanations and reasons beyond avoiding fine and punishment.

Approaches to address implementation challenges

Participants suggested some approaches to address the challenges presented in the previous section, based on the area of their work and their expertise. Some of

the suggestions are very specific, and we try to explain them in the context of the discussion. **A group of experts**: building a group consisting of legal and technical experts was suggested by E3 and E4. Both argued that addressing GDPR-related challenges is not simple and therefore can not be expected to be done only by single individuals. E4 suggested to include *'lawyers, data processors, those who are aware of how information flows in a company, IT people, data ethics experts, those with humanistic training, or philosophers, or those who have legal ethics as their main concern, so this should be a multidisciplinary discussion'*. The communication among members of such a group can also be challenging, and E3 suggested that assigning one individual with knowledge in both legal and technical aspects of development process could be a way to facilitate the communication.

Customised guidelines: All experts agreed on the importance of developing a specific guideline for each company or service provider. E1 said: *'there has to be a guideline for designing interactive systems, that is fundamental, this is technical, then it is the discussion of system requirements that must be designed with features supporting the implementation of GDPR, then you need certain visual and graphical pallets based on companies visual brand, that is related to companies design guidelines'*.

Contextualisation: The best way to communicate concepts related to privacy to users is through simplified but tangible methods (i.e. mentioned by E1, E2, E3 and E5). E1 calls it *wise notification*, and E3 believes that if the consent is not fully understandable for users, then it can turn into a tool for service providers to obtain permission for processing user data without protecting the users' privacy.

Integrating GDPR considerations into the development process

Regarding the phase in which one should consider GDPR compliance factors, all experts agreed on the importance of considering GDPR compliance factors at the requirement gathering and analysis stage or even prior to that. E1 said: *'it should definitely be discussed at requirement analysis and design, but it should also stay through the other stages'*. This is in line with GDPR's suggestions which encourage service providers to follow privacy by design principles and include privacy considerations in early and all stages of system development (Leda Bargiotti, Inge Gielis, Bram Verdegem, Pieter Breyne, Francesco Pignatelli, Paul Smits Ray Boguslawski, 2016). We also asked the participants who is responsible for the GDPR implementation. While all agreed on assigning a group of individuals with various expertise as responsible for GDPR implementation is the best strategy, a few believed that the implementation is the service providers' responsibility rather than developers and designers (i.e. mentioned by E1, E2 and E3).

4.5 Guidelines for realising GDPR-compliant implementations

As mentioned in Section 4.1, the GDPR does not come with explicit guidelines for developers and designers to help them implement its requirements. This need for guidelines was confirmed during the expert interviews (see Section 4.4.3). With focus on Notice, Consent, and Control (NCC) factors from GDPR, presented in section 4.3, We developed a set of guidelines. In order to construct a guideline that is easy to follow, we defined two primary stages for developers (see Fig. 4.2); Content stage, which refers to the body of the material that should be included for addressing each of the factors (e.g. the purpose of processing should be stated when designing for Notice). Also, the communication stage which includes suggestions about how to communicate the content to users (e.g. text or icon).

The content stage is about "What" to include, and it covers a few aspects; first, developers and designers should understand what each of these factors mean. And second, what to include when designing for Notice, Consent, or Control. The content stage is designed based on GDPR's main document (EU, 2016) to cover the list of requirements for addressing NCC factors. This stage provides a list of required information that should be provided to users.

Communication stage is about "How" to communicate, and focuses on the aspects regarding the communication of the body of the material produced in the Content stage. This stage addresses aspects such as appearance and characteristics of the NCC factors (e.g. when to ask for users consent and how should that look like). Communication stage includes the suggestions from experts for designing the content and appearance for NCC factors.

The guidelines listed in Fig. 4.2 should be used together with the explanations for each factor presented in section 5.1, 5.2, and 5.3. Regarding the content that one should create for addressing GDPR's requirements, there are repetitions for NCC factors which are purposes of processing, Recipients, Retention, Existence of profiling for all three, Data transfer for Notice and Consent, Existence of the right for control for Notice and Control. The reason that this work has not presented them all together is to emphasise the legal requirements for each, and also to highlight that although the content created for them could be reused but it should also be adjusted for each factor. For instance, the content created for Notice does not require the confirmation from data subjects as Consent, therefore, despite the similarity of the content, the way of rephrasing and presenting might be different.

In the following subsections, we will describe all the factors incorporated in the guidelines. We will start by introducing those relating to Notice, then move on to those connected to Consent and we will finish by defining factors linked to control. Each subsection is split into the two stages we described above. Fig 4.2 provides an overview over all factors and stages.

Stage one, "What to communicate" (legal requirements for creating content)		
Notice	**Consent**	**Control**
N1.1. Controller's information N1.2. DPO 's information N1.3.Purposes of processing N1.4. Lawful processing N1.5. Recipients N1.6. Data transfer N1.7. Retention N1.8. Existence of the right for control N1.9. Consequence of not providing the data N1.10. Existence of profiling N1.11. Disclosure of personal data breaches	C1.1. Purpose of the processing C1.2. Recipient C1.3. Data transfer C1.4. Retention C1.5. Existence of profiling C1.6. Renew C1.7. Withdraw	CO1.1. Access to collected data CO1.2. Purpose of the processing CO1.3. Recipient CO1.4. Retention CO1.5. Existence of the right for control CO1.6. Existence of profiling CO1.7. Rectify CO1.8. Erasure CO1.9. Restriction CO1.10. Object
Stage two, "How to communicate" (experts suggestions for design and communication)		
Notice	**Consent**	**Control**
N2.1. Discuss Notice in all stages N2.2. Balance quality and the quantity of the info N2.3. Precise and understandable N2.4. Accessible info N2.5. Avoid long text N2.6. Use visuals	C2.1. Discuss and Design Consent C2.2. Clear statement C2.3. Withdrawal consequences C2.4. Conceptualising the content C2.5. Contextualising the content C2.6. Clear parameters C2.7. Clear statement	CO2.1. Access type CO2.2. Direct access CO2.3. Wise access CO2.4 Opt-Out CO2.5. Clear statement

Fig. 4.2: guidelines recommendation based on legal requirements and expert suggestions.

4.5.1 Notice

Content stage - Notice (N1)

Users should be informed about all activities related to personal data processing such as data collection, its purposes and data breaches. When creating the content for Notice, developers and designers should include the information listed in the first column of Figure 4.2. *Controller's information* (**N1.1.**) refers to the identity and the contact details of the data controller. *DPO 's information* (**N1.2**) refers to the contact details of the data protection officer. *Purposes of processing* (**N1.3**) explains why personal data is collected and what is being done with it. It should also be made clear that the processing is lawful, meaning that it should meet the requirements explained in Art. 6 for *lawful processing* (**N1.4**). Another crucial aspect is to communicate to users to whom the personal data is going to be disclosed – its *recipients* (**N1.5**). These can be, for example, a natural or legal person, public authority, agency or another body (who is going to see the collected data or have access to it). *Data transfer* (**N1.6**) refers to whether any personal data is transferred

to a third country or international organisation (where are you going to send it). *Retention* (**N1.7**) describes the period of time for which the personal data will be stored, or if that is not possible, the criteria that will be used to determine that period. (for how long are you going to keep the collected personal data). A further important piece of information is the *existence of the right for control* (**N1.8**). This relates to the right to request from the controller all aspects of control meaning the right to access, rectify or erase personal data as well as to restrict processing or to move data to another provider. Data subjects also have to be informed after such a request has been processed. (what are the rights of data subjects about their personal data). Consequence of not providing the data N1.9 refers to whether data subjects are obliged to provide personal data and of the possible consequences of failure to provide such data. (does the data subject have to provide personal data? what will happen otherwise?) Existence of profiling N1.10 relates to the existence of automated decision-making, including profiling. The information should clearly explain the logic underpinning the decision-making, as well as the significance and the envisaged consequences of such processing for the data subject (Is there any profiling activity involved? why? what does that mean?) Disclosure of personal data breaches N.11 refers to communicating personal data breaches to the data subject in particular when the personal data breach is likely to result in a high risk to the rights and freedoms of natural person (EU, 2016).

Communication stage - Notice (N2)

After creating the content for Notice, it is important to decide how to communicate it with users. Recital 60 of GDPR (EU, 2016) states that the information provided for data subjects *'may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing'*. The recital's description can be interpreted differently in various context. During the expert interviews, we asked about the best time and the most appropriate way to notify users. A list of keywords regarding experts' opinions is presented in Figure 4.2. Discuss Notice in all stages N2.1 suggests that designing the Notice should be discussed and addressed through requirement gathering, design criteria, design and development phases. Balance quality and the quantity of the info N2.2. propose to pay attention to the importance of balancing the quality and the quantity of the information they present in Notice, developers and designers should decide about how much information must be shown which while it is short, it still gives a profound overview. Precise and understandable N2.3 refers to the need for using simple, understandable and relevant terms instead of complicated, legal or technical ones. Accessible info N2.4. suggest that the information presented through Notice should be accessible later (e.g. through setting) and it should not be ephemeral (e.g. to be shown only when installing the application). Avoid long

text N2.5 suggest that the message should be communicated through a short and wise text. Use visuals N2.6 propose to prioritise the use of visual means and relevant Icons over using text. Visual reminders N2.7 refers to not only presenting the information through visual means but also encourages the use of visual reminders to communicate the information to Users fully.

4.5.2 Consent

Content stage - Consent (C1)

The GDPR requires user's Consent to data processing activities. Those who collect and process the data must be able to prove that the Consent was given. What user is going to consent to should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms - Recital 42. Regarding the content of the Consent, there are a number of overlapping points with the information listed for the Notice as the focus is on the data processing activities. Purposes of processing C1.1, Recipient C1.2, Data transfer C1.3, Retention C1.4, and Existence of profiling C1.4, correspond to (**N1.3**), (**N1.5**), (**N1.6**), (**N1.7**), (**N1.10**) from section 4.5.1. The key difference is related to formulating the content: for Notice, the purpose was only to inform users, but for Consent, the goal is to ask for the explicit agreement to data processing activities. Beside consenting to the data processing activities, Consent has two specific conditions as well. GDPR requires to Renew C1.6 the Consent if the purpose of the data processing changes, the Consent must be renewed, and information should be presented to users accordingly. Also, users shall have the right to Withdraw C1.7 their consent at any time and through easy means Art. 7 (EU, 2016). It is important that users have been informed about the right of withdrawal prior to consenting.

Communication stage - Consent (C2)

We discussed consent during the expert interviews. The main concern, which was raised by all experts, was the challenge of assuring that the presented information (e.g., text or image) in Consent is understandable for non-technical users. In other words, how to make sure that users know what are they consenting to and are aware of the consequences of such consent. Experts suggest that for designing a Consent that conveys a comprehensible message to users, it is important to Discuss and Design Consent C2.1 through various development stages such as requirement gathering, design and, evaluation. They also suggest that the developers and designers should provide clear statement C2.2 explaining that the user will have the opportunity to change her/his decision regarding the consent later, also explain

how and through which steps one can make such changes (i.e. withdrawal right). Additional important information that Consent should include according to experts is regarding the consequences of withdrawing consent, withdrawal consequences C2.3 should clearly state the outcome of user's decision after withdrawal. Expert suggest to conceptualising the content C2.4 for users by telling them how developers will use that data rather how they will *not* use the data might have a better result. Furthermore, contextualising the content C2.5 through everyday life events of users can also be a way to make it understandable. Experts also encourage designers and developers to use clear parameters C2.6 explaining to what users are consenting to, and clear statement C2.7 explaining who will market their data to.

4.5.3 Control

Content stage - Control (CO1)

Control consists of the factors described in the GDPR as users' rights and obligations to provide them with controls over their personal data. The factors are access, rectification, erasure, restriction of processing and object (i.e. explained in details in section 4.3). In summary, Control should provide to users; access to the collected data, the possibility of updating the collected data, and also an option to opt-out from data collection activities. Regarding the content of the Control, the same as Consent, there are a number of overlapping points with the information listed for the Notice but the key difference is the way of providing them to users, for example, providing the information regarding the collection of data will not be sufficient, and it should be followed by the possibility of opt-out from data collection. The similar content from includes Purposes of processing CO1.2, Recipient CO1.3, Retention CO1.4, existence of the right for control CO1.5, and Existence of profiling CO1.6, correspond to (**N1.3**), (**N1.5**), (**N1.6**), (**N1.7**), (**N1.8**), (**N1.10**) from section 4.5.1. In addition to the listed information, there are a few controls that are explicitly required by GDPR to be provided to users; Access to collected data CO1.1 which gives users the right to access the collected personal data and also to obtain a copy of the collected information from data controllers. Also, users have the right of Rectify CO1.7 or Erasure CO1.8, which means the personal data collected about them can be rectified or be erased and no longer processed, particularly when the data is no longer necessary for the functionality of the service or users have withdrawn their consent. In addition, users have the right to ask for the restriction CO1.9 of the processing and the right to object CO1.10 to processing in the case of direct marketing including profiling.

Communication stage - Control (CO2)

This section summarises the experts' opinions on how to address control. The main concern when discussing the Control was related to the possibility of increased interaction complexity for users which could be resulted after providing controls over their personal data. Thus, experts suggest avoiding such complexities by explaining the Access type CO2.1 to users, meaning, the kind and degree of the access should be communicated to users through Notice and Consent. Also, the Direct access CO2.2 should be given to the users with easy possibilities of updating and observing the collected data about them. Also, users should be notified about the consequences of erasing the data (e.g. erasing the data can influence the functionality of the service they use) - Wise access CO2.3. If users request Opt-Out CO2.4, the collection process has to be stopped, and this change should be communicated to them. The success of this operation has to be reported back to the users so that they can confirm that data is no longer collected. The opt-out option should be directly accessible through the application but similar to other decisions like erasing the data; there is a need for clear statement CO2.5 about the consequences of enabling Opt-Out.

4.5.4 Applying the guidelines during development

Software engineering lifecycle for developing products includes Requirement analysis, Design, Development, Test, Implementation, and Maintenance (Medicare & Medicaid Services et al., 2008). The majority of the experts stated that while it is essential to consider addressing privacy-related issues in all stages of the service development, there should be more attention on addressing these issues during requirement analysis, design and development stages (i.e., in line with privacy by design principles (Cavoukian, 2009)). The following is a summary of suggestions that each of these stages can include for addressing GDPR requirements at UI level.

Requirement analysis stage: this stage could include *awareness and education* which refers to the need of educational programs for designers, developers, and everyone in the development team who is involved in the collection, use or the process of personal data on three subjects; 1) GDPR regulations, particularly data subjects rights. 2) The ethical and philosophical reasoning of protecting individual's data privacy and, and 3) the consequence of noncompliance for the company. It is also essential to perform *information flow inspection* during the requirement analysis stage for understanding how the data flow works, mainly for finding gaps (i.e., which part of the information flow requires GDPR compliance) and then designing solutions.

Design stage: with respect to the activities and findings from the requirement analysis stage, could *identify the points* in the development cycle that GDPR requirements should be addressed (i.e., which starts from the result of the information flow

inspection). When the addressing points are clear, then it would be helpful to map the requirements to tasks and assign them to a group of individuals with various expertise, such as developer, designer, DPO, lawyer, ethics advisor. This stage could also develop an action plan connecting GDPR requirements to system development life cycle based on every particular product's goal.

Development stage: while initial design ideas have developed in the design stage, development stage is where the full content (i.e. the information that should be included in the body of the solutions) and design (i.e. the way that solutions should be communicated to users) of the NCC should be finalised.

4.6 Guidelines in practice: a take-home study

In order to evaluate the use of the guidelines during actual software development, we asked developers to use it during nine-weeks projects. Our main evaluation goal was to see whether developers could use the guidelines to incorporate (location) privacy features into newly developed location-based services. We were also interested in any problems they encountered and what they thought about the guidelines. For this purpose, we tasked the four participants of a nine-weeks project course at our department (i.e. student developers) with the design and development of an LBS.

4.6.1 Participants

All participants were students at one of the two Master programmes offered by our institute. Programming skills varied amongst the participants, with three being quite experienced and one of the intermediary skills. The four students had between 3 and 20 years of programming experience, had participated in up to ten programming courses and rated their own experience between 4 and 10 (10 being the highest mark). Regarding the concerns about location privacy, two participants were quite concerned about sharing location information (scoring 20 and 18 out of a maximum of 30). The two other students were less concerned (scoring seven and nine out of the maximum of 30.).

4.6.2 Materials and Procedure

The student developers were instructed to use an existing framework (LBS engine[2]) together with the guidelines introduced in section 4.5 to build example LBS that comply with GDPR. The LBS engine is a *toolkit* in the sense of Olsen, 2007 as it

[2]https://github.com/LEinfeldt/LBS-Engine

provides a template which helps design location-based services. Asking participants to create example apps within about three months is a strategy for toolkit evaluation called *take-home study* Ledo et al., 2018. This approach is useful to gather some evidence on the external validity of the used tools (LBS engine and guidelines). We used the System Usability Questionnaire (SUS, see Brooke, 2013 for a recent review of its properties) to evaluate the usability of the LBS engine and the guidelines.

Over a period of nine weeks, the four student developers were split into two teams. They were tasked with designing and developing two fully functioning LBS prototypes of their own choices while using the GDPR guidelines and the LBS engine. They received short introductory lectures about both tools at the beginning of the course. Their main task was to conceive and implement a functional LBS. In addition, we briefed them on the GDPR guidelines and asked them to consider these during development. At the end of the study, we used the SUS test to evaluate the guidelines and LBS engine. In order to assess the effectiveness of the guidelines, we also analysed the privacy-preserving features of the developed LBSs by examining the final submitted products as well as their weekly progress reports.

4.6.3 Results

In the following, we summarise key results of the take-home study: the implementations that were produced, the privacy features that were implemented, insights into how the guidelines were perceived and used, as well as challenges and limitations we observed. While all developers received the same information, the systems and features they implemented to address location privacy varied considerably between the two teams.

Implementations

The two teams of two students each developed two very different LBS: GeoFreebie and TourChamp. GeoFreebie[3] is a location-based mobile application that helps users find and donate gifts by visualising items on a map. It is based on the idea of 'freecycling' – recycling by giving unneeded items away to other people for free. The app provides a spatially ordered list for users to search for free items. Furthermore, GeoFreebie can notify users about gifts in their current vicinity (see Fig. 4.3). Gifters can upload their donation data without giving their exact location in order to protect their privacy.

TourChamp[4] is a location-based service for newcomers to a city to find tourist spots and then test their knowledge about the new places they visit. The users can

[3]https://github.com/lbraun/geofreebie
[4]https://github.com/TeKraft/TourChamp

use the application map to identify tourist spots in a city with the possibility to take part in a multiple-choice quiz about these spots (see Fig. 4.4).

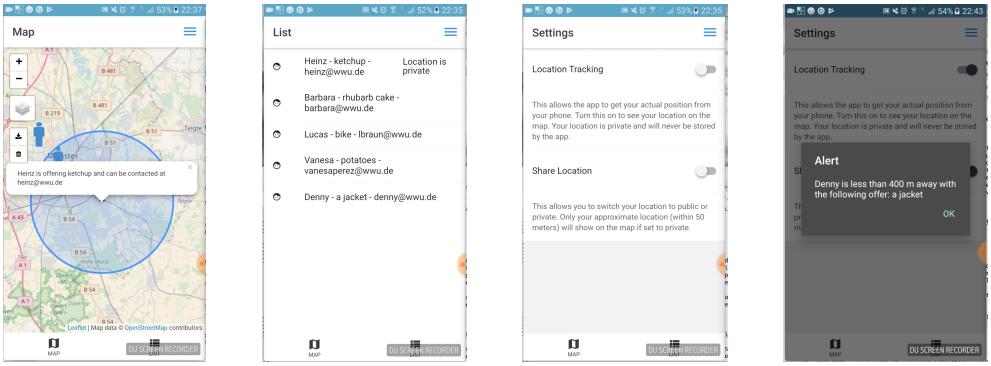


Fig. 4.3: GeoFreebie (left to right): a)Approximate location of the users shown in a blue circle, b)marked location info as private, c) setting options to adjust location tracking and location sharing, d) notification pop-up if the location sharing and tracking are enabled.

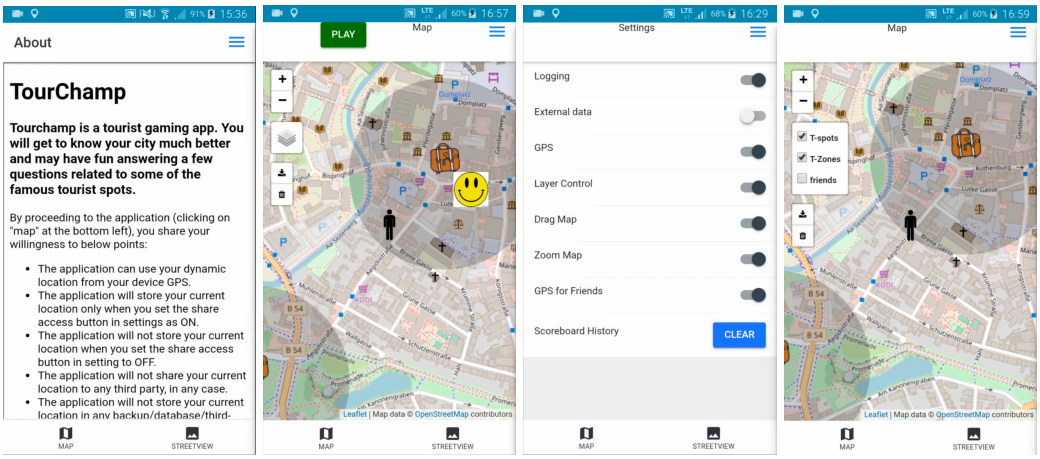


Fig. 4.4: TourChamp (left to right): a) Notice, b) visual indications of friends presence when location sharing is enabled, c) setting options to adjust location sharing (GPS) for public or only friends, d) layered setting adjustment to enable/disable location sharing.

Location Privacy Features

Both teams were encouraged to discuss location privacy from the beginning of the process. They reported on such discussions during their progress meetings. At the beginning of the course, they believed their applications could harm users privacy in any way. They changed their mind after learning about the possibility of extracting personal data from location data combined with other types of data. Both teams implemented some privacy-preserving measures while developing the architecture, but they were finalised during the development and UI design stages.

Geofreebie's developers hid the current user location by default. In the list view, the location information of the users who are not willing to share their location was marked as private. Even when this option was enabled, only an approximate location

of users in a zone (i.e. buffer) is shown, therefore avoiding the exact location of users[5]. The app settings screen provides users with two specific options, one for location data tracking and one for location data sharing. There are further means for users to communicate with each other (e.g. a phone number or an email address). Application users can thus reach their goal without disclosure of their location data. However, enabling location sharing and tracking benefits users by providing pop-up notifications when they are close to a gift (Fig. 4.3). Geofreebie's developers designed a notice explaining how the app works and also explaining that users are in control of sharing their location. The notice implemented features N1.3 and N1.8 of the guidelines. They also provided controls for users, giving them the possibility of opt-out from location tracking and data sharing. Their implementation covered CO1.2, CO1.9, and CO1.10 of the guidelines provided in Fig. 4.2. Geofreebie's developers also explicitly avoided making users exact location publicly visible. These features were implemented to build a GDPR-compliant LBS prototype.

TourChamp's developers designed a notice in the form of text explaining that location privacy can be adjusted through the settings (i.e. N1.3 and N1.8). The setting screen provides options for users to enable or disable the GPS, which will impact the location sharing directly (i.e. CO1.2, CO1.5, CO1.9, and CO1.10). Another feature in the setting is GPS for a friend. Disabling this option will stop sending users location to the server but also will influence the social aspect of the game meaning that user will no longer be able to see other players (i.e. yellow happy faces) and has to continue the game individually. To adjust location privacy and stop location sharing, users were provided with an option in the main screen of the app, namely the layers button. Unchecking the friend layer (see Fig. 4.4 d) will disable the location sharing of the users with others, similar to the controls available in the setting menu (i.e. fine-grained adjustment for enabling and disabling GPS for public and friends or based on different zones), (see Fig. 4.4 c).

In addition to these features for complying with GDPR, Tourchamp's developers also designed and answered a set of questions for addressing location data privacy. The questions were: "*What data we collect from the user? - How do we store it? - Is it prone to a breach? - Is the user aware of the data collection and storage? - Can the user withdraw/delete the shared data? -Is a user consent taken while getting data?*", through these questions they covered a discussion (i.e. did not implement as features) on a number of items from the guidelines such as N1.7, CO1.7, and CO1.8. Fig. 4.5 shows each application and the addressed features from the guidelines. We found this technique an interesting interpretation of the proposed guidelines and in general a useful strategy to consider location privacy during the process of developing privacy-aware and GDPR-compliant LBS. It was expected to observe that the implementation of the guidelines has been very different for both teams. Leading to the conclusion of the need for including some level of flexibility while developing such guidelines.

[5]The technical term for this technique is *obfuscation* (see, e.g. Duckham and Kulik, 2006)

The features that none of the teams addressed were related to consent. The reason could be related to the developers' assumption that Consent should be addressed during the installation process (e.g. end user agreement). Although GDPR explicitly requires Consent to be an active part of the application, the developers' decision in this study could be an indication that the matter of addressing Consent needs further exploration (i.e. when and how to ask for user's consent).

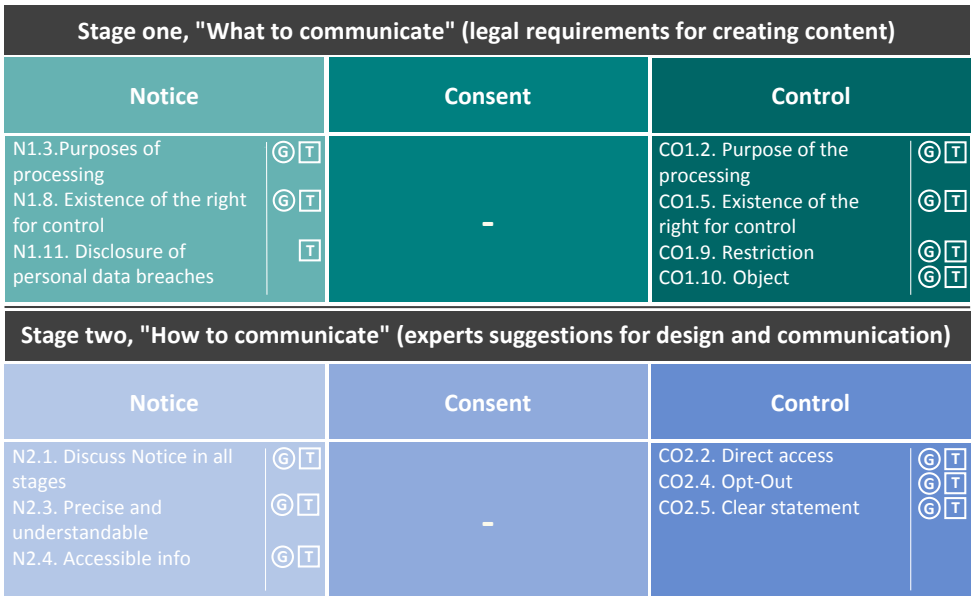


Fig. 4.5: guidelines recommendation reflected in the two LBS developed during the take-home study: 'G' and 'T' indicate factors that were realised in the GeoFreebie and TourChamp LBS, respectively.

Guidelines usability

We used the System Usability Scale (SUS) (Lewis and Sauro, 2009) for measuring the usability of both the LBS engine and the guidelines. In order to clearly distinguish what was being evaluated, we replaced the word 'system' with 'GDPR guidelines' in the SUS form.

We are presenting only the results for the guidelines here due to the overall focus of this article on location privacy rather than rapid prototyping of LBS.The SUS results show that the perceived usability of the guidelines varied between developers: the SUS score (Brooke et al., 1996) of the participants ranged from 35 (P2) over 55 (P1) and 65 (P4) to 72.5 (P3). The Mean SUS score was 56.9 for our study. According to the adjective rating scale proposed by Bangor et al. (2009)'s (with a SUS score of 12.5 corresponding to 'the worst imaginable' usability and a SUS score of 90.9 representing 'the best imaginable' one), we can conclude that the overall perception of the guidelines was 'OK' (i.e. higher than 50.9). Due to the low number of respondents, individual scores (e.g. the rating P2 gave) had a disproportionate impact on the mean score. While this result thus provides initial evidence that

developers can use the guidelines, it also indicates the need to run further usability tests (involving a higher number of developers) in order to spot usability issues as well as to refine the guidelines and their presentation.

Limitations and Challenges

The take-home study provides some initial insights into how the guidelines can be used to work towards GDPR-compliance during LBS development. However, only four developers were involved in an academic setting. Using more developers in a commercial setting over a longer period of time would have led to deeper insights regarding trade-offs between privacy and other constraints. Nevertheless, the study showed that developers could use the guidelines during the development of a location-based service that incorporates (location) privacy-preserving features.

The study also revealed some challenges for the guidelines. The relatively low SUS scores and informal feedback indicate that the developers were struggling with the guidelines. We attribute this to the overall complexity of the legal framework as well as its generality. However, the diversity of the two developed system also highlights the need for the latter. One way to address the issues mentioned above could be to develop an interactive toolkit (or Wizard) that makes it easier to identify relevant factors and potential solutions at specific points during the development process.

4.7 Discussion

In the following, we briefly discuss key aspects relating to the GDPR and our guidelines, point out opportunities for future work, and review the limitations of our work.

4.7.1 Implications and Observations

The guidelines described above are based on a thorough analysis of the legal text as well as on input from experts. Our take-home study provides initial evidence that they can help designers and developers in designing UIs that provide information and interaction along the lines of what the GDPR requires. The LBS that were produced by the developers participating in our study all included features to improve the location-privacy of their users. While the guidelines were effective in this respect, we also found that their usability leaves room for improvements.

Many of the technical aspects included in the GDPR are more familiar to developers and are more easily mapped to technical solutions (such as using strong

encryption). By separating user-facing from technical requirements (such as secure storage of personal data), the guideline has the potential to make it easier for developers to create LBS that comply with GDPR. Though both types of requirements need to be tackled for full compliance, we only evaluated one type (user-facing requirements) in this article.

In addition, the guidelines can serve as a way to communicate between different stakeholders in the development process (designers, developers, data protection officers, legal experts, users). The guidelines are in line with Privacy-by-Design principles (Cavoukian, 2009) and support the paradigm shift that GDPR tries to enforce, namely pro-activeness with respect to privacy protection (rather than re-activeness). Since GDPR *redefines the context for interactive development and use*, the discussion provided in this article contributes to make the peculiarities of this context explicit. Therefore, they are one way of further specifying the *activity context* dimension of Döweling et al. (2012)'s model of interactive system design.

4.7.2 Future work

The analysis presented earlier and the proposed guidelines can serve as a basis for much future work on interactive system design including LBS. They can inform future efforts which try to standardise UI designs relevant to the context of GDPR. For example, they could be used to design a standard user interface that controls how location information is shared in a location-based service. In addition, the proposed guidelines could be a starting point for developing a formal model that encodes specific aspects of the GDPR and then facilitates (semi-)automatic proofs of compliance (Ivory and Hearst, 2001). However, given the complexity of the legislation and the topic in general, realising a comprehensive and consistent *formal* model of the GDPR appears to be a quite challenging task. As mentioned above, creating an interactive tool for developers that provides and guides access to the guidelines might be a promising (and complementary) alternative to a formal model.

Finally, the presented guideline points at the need for further research into three areas: effective ways of communicating privacy notices, user-friendly techniques of getting privacy consent, and truly enabling user control over their data. Previous research has already produced a design space for effective privacy notices (see, e.g., Schaub, Balebako, et al., 2015), but more work is needed to articulate design spaces for UI elements which are best suitable while requesting privacy consent and control in interactive systems.

4.7.3 Limitations

Our work is subject to several limitations. The most important one is arguably that the proposed guidelines cannot guarantee that the resulting services will fully comply with the GDPR. This is mainly due to the guidelines only covering a subset of the GDPR (i.e. those aspects that can be addressed at the UI level). In addition, the guidelines are at a level of abstraction that allows a broad application to different systems, which prevents very specific instructions that could be unambiguously checked. Nevertheless, we argue that the guidelines are a useful abstraction of the legal text that provide designers and developers with guidance towards realising a GDPR-compliant service. Although our evaluation took place during the actual development of two LBS, it was clearly limited in terms of length, the number of participants and the diversity of applications that were developed. Nevertheless, it provides initial insights into how the guideline is used during development.

Furthermore, the article has not discussed responsibilities when it comes to actually realising these guidelines in practice. The challenge of who is responsible for implementing GDPR was also one of the discussion points in the interviews. E3 and E7 agreed on the strategy of bringing together a group of individuals, developers, designers, ethical advisers and service providers. On the other hand, E1 believed that "*this (i.e. compliance with GDPR) is not designers' responsibility, the one who is responsible for the project is also the main responsible person for GDPR compliance first*". In the view of E2, the government should take the responsibility for the implementation of GDPR in both public and private sectors while E3 had a different opinion, mentioning that GDPR implementation requires hiring data protection officers (DPO), and stressed that "*they are going to be the main channel of communicating with data protection authorities...*". It is acknowledged here that the question "who will implement the guidelines?" is important for GDPR-compliant services, but that question is not discussed further in this article since it involves institutional concerns which are not the main focus of this work.

4.8 Conclusion

Privacy legislation such as the General Data Protection Regulation (GDPR) can be a big challenge for developers who have to implement systems that comply with it. Understanding the legal text already requires a lot of effort, but legal frameworks also do not include specific instructions for how to realise compliant software. In this article, we report on work to address this gap between the legislation and the implementation, with a particular focus on location privacy and location-based services. We analysed the legal text of the GDPR and extracted key aspects (i.e., challenges and approaches) relating to creating compliant LBS.

In addition, we carried out interviews with experts to identify key challenges and issues developers face when building privacy-aware software. Based on the outcomes of the analysis and the interviews, we create guidelines for designers and developers to help them create systems that comply with the GDPR. In our work, we focused on location data and legislation aspects that require user interaction (i.e. privacy regulations that relate to the user interface). The guidelines are grouped into two stages (what to communicate and how to communicate it) and into three groups (Notice, Consent, Control) that are directly derived from the GDPR.
The usefulness of these guidelines was demonstrated through their application to the development of an interactive location-based service in a take-home study. The guidelines can inform the standardisation of GDPR-compliant user interface (UI) designs such as a dialogue for location sharing that includes all necessary functionality and visualises all legally required information. In addition, the guidelines can be used by developers as a starting point for their work on GDPR-compliant services.

4.9 Appendix A - Summarised analysis of NCC factors

4.9.1 Notice

GDPR requires the ensuring of lawful, fair and transparent processing of personal data. According to the recital 60 of GDPR EU, 2016, the processing is fair and transparent if the data subject is informed of the existence of the processing and its purposes. The controller should provide data subjects with the information that is listed in Art. 13 of GDPR regarding personal data collection from the data subject: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second sub paragraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. In addition to the list, data subjects should also be informed about: (a) the period for which their personal data will be stored, or if that is impossible, the criteria used to determine that period; (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; (c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (d) the right to lodge a complaint with a supervisory authority; (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject Art.13 - EU, 2016.

As mentioned in the previous paragraph, data subjects should be informed in the case of profiling, but according to recital 60, data subjects should also be informed about the consequences of both accepting the processing and objecting to it in the case of profiling. Data subjects should also be informed if any data breach occurs, according to Art. 34: *'when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay'*. The subjects should also be instructed to take steps to mitigate the damage after the communication of the incident - EU, 2016. Informing data subjects about their rights, the consequences of their decisions and the activities of the controller can ensure fairness and transparency regarding the lawfulness of the processing. GDPR considers the processing lawful if "*the data subject has given consent to the processing of his or her personal data for one or more specific purposes*" or processing is necessary for various reasons such as " *compliance with legal obligation*" or " *for the performance of a task carried out in the public interest*" Recital 60 -(EU, 2016). Article 19 adds another aspect to the list of information that data subject should be informed about, namely *The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it*.

4.9.2 Consent

According to the GDPR, consent is one of the fundamental principles to make data processing activities lawful. Article 4, defines consent of data subjects as *any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her* EU, 2016. Article 7. defines conditions for the consent such as (1) where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data and (2) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. Recital 42 also lists some requirements for consent: *for consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment*. The consent should communicate the processing activities with data subjects which is similar to

notice, but the primary difference is that the consent requires active approval and confirmation from data subjects. It also needs to be flexible to support the features of withdrawal (i.e. the right of opting out from data processing) and renewal (i.e. receiving an updated consent when the purpose of the processing has changed).

4.9.3 Control

GDPR stresses the importance of providing data subjects with control over their personal data. Control includes various principles such as the right of access, the right to rectification and erasure, the right to restriction, the right to data portability and the right to object. We will briefly explain the legal requirements for each.

- Access - according to Art. 15: The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source; (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

- Rectification - Art. 16: The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

- Erasure ('right to be forgotten'): The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the

personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

- Restriction of processing - Art. 18: The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; (b) the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

- Data portability - Art. 19: The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided Art 20.

- Object - Art. 21: The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

5 Discussion

> *In the twenty-first century our personal data is probably the most valuable resource most humans still have to offer, and we are giving it to the tech giants in exchange for email services and funny cat videos.*
>
> **— Yuval Noah Harari**
> (Homo Deus: A Brief History of Tomorrow)

This chapter begins with a general discussion about data privacy; it will then discuss location data privacy in particular with respect to the guiding questions as well as the connections between the presented approaches in this thesis. The summary of this chapter will highlight the points that resulted from addressing the main research question. The summary will also discuss the challenge of evaluating (location) data privacy.

5.1 The challenging matter of data privacy protection

As discussed in previous chapters, many services are in the need of using location data to provide relevant information to their users. Location data is about the actual and physical location of individuals. If this data is combined with other types of data such as health or financial data, it can provide an excellent source to not only identify individuals whereabouts but also extract sensitive information about them (e.g. their interests, habits, consumption patterns and even an estimation of their future behaviours) (Altman et al., 2018). This highlights the importance of protecting (location) data privacy. In a world where data is the *new oil* (Economist, 2017) , the commercial values of location data are significant (BIA/Kelsey, 2016). The commercial value of collecting personal data motivates many companies to collect and store as much personal data as possible when they have a chance of doing so. The data collection can happen through simple applications on smartphones, which now exist in almost every individual's pocket. It seems that arguing for limiting the personal data collection for protecting data privacy falls into a situation similar to

when environmental organisations struggle to limit the oil extraction to save the environment. Where negative societal effects compete against positive commercial values.

Smartphones has given a high level of comfort to the everyday lives of their users, but smartphones are also one of the best tools to facilitate surveillance by using the phones features for continuous tracking of individuals (Tsukayama, 2018). Maybe one of the most important reasons that make the protection of data privacy challenging is the opportunity that technological advancement has created. The pervasive use of smartphones, "*spies in our pockets*" (Temming, 2018), have created an opportunity for mass surveillance. Throughout the history, it has never been so easy to have the possibility of mass surveillance without regard to physical distance. Everyone from a hardware provider and cell tower controller to an app developer or a hacker has the chance to collect personal data. Surveillance can cause severe threats and risks to human rights (Harding, 2015) in all types of societies, "*constant surveillance of citizens' locations can be used as a tool for oppression and to limit freedom of speech, even in democracies*" (Keßler and McKenzie, 2018). The usage of mass surveillance is often justified with reasons such as preventing terrorist attacks and increasing personal safety (Deeyfuss, 2017). For such reasons, the negative implications of mass surveillance on individuals lives receive little or no attention. This leads to a moral dilemma where individuals might feel pressured and stop valuing their rights for data privacy protection in order to not interfere with the process of fighting organised crimes or terrorism.

Protecting privacy is going to be even more challenging due to the culture of so-called "sharing is caring" (Eggers, 2015). Sharing is caring culture encourages individuals to share every moment of their private life with others. Individuals who want to keep part of their life private could be blamed for not caring for others by not contributing or withholding information, from which the collective *could* have benefited. Despite all the difficulties on the way of protecting data privacy, there is still hope to do it. Many parties have the power to change the course of the current practices, and many are already are taking steps towards that direction. These include researchers, scientists, data ethic activists, and technology providers (Altman et al., 2018). Works such as *teachprivacy.com* [1] are working towards increasing the awareness regarding data privacy. Some governments, such as the European Union, has also taken action and has shown that data privacy matters enough to update laws and establish regulations to protect the personal data of their citizens. The General Data Privacy regulation EU, 2016, which entered into force recently is a good example for addressing data privacy related issues, but GDPR in its current shape includes many uncertainties regarding service providers and developers responsibilities (Raschke et al., 2017).

[1] http://teachprivacy.com/

This work aims at developing various means for protecting (location) data privacy. The following sections will discuss location data privacy in the process of LBS development. It will also discuss the proposed approaches and their connection to the guiding questions.

5.2 Addressing Location Data Privacy

Addressing (location) privacy is a matter that should be considered through all stages of LBS development (i.e. from early ideation to the moment that users' location data is collected, stored or discarded). In order to discuss the implementation of location privacy protection measures, this work has separated the stages and the roles of those who are responsible for such implementations. While there has also been suggestions and studies involving end users' preferences in this context, the primary emphasis has been on the responsibilities and opportunities that the developers and designers of LBS have regarding the addressing and implementation of location privacy protection measures in all the stages of the development process. The goal has been to show how addressing location privacy can eventually become a natural part of the service development requirements and not only a side issue to consider during the final stages of LBS development.

5.2.1 LBS Architecture to manage location privacy

In order to answer GQ1 , "*How should location information be managed in LBS to protect location privacy?*", this work, proposed a model for developing LBS architecture based on the Privacy by Design (PbD) approach. This model extends existing LBS architectures with two new components with the focus on the management of location data in a privacy-protected manner. Chapter 2 suggested to add two new components to the architecture of LBS, one dedicated to the decisions regarding the storage of the location data right after its collection (i.e. location privacy management (LPM)) and one dedicated to the controls provided for users to manage their location privacy based on individual preferences (i.e. location privacy user interface (LP UI)).

In order to illustrate how ephemerality can be implemented and used in everyday life, a team of student-developers during a study project, have developed a prototype. The prototype is called *Happy Share*, and is a service designed to enable users to share their experiences with other people in the same area while visiting or exploring a city (e.g. during events such as fun fairs or festivals). The application provides means to share short messages anonymously with people in the same geographic area. In addition, it enables users to define an expiration time for each message. The

system does not store any location data of the users, nor does it store their messages over time. Happy Share has two main components: a server component and a client component. The server component[2] enables the user to define zones, their spatial extent, their expiry time as well as their topics. The server component also offers the possibility of getting statistics about activities happening within a zone (see Figure 5.1). The fact that a zone has an expiry time is a feature supporting temporal ephemerality at the data level (a zone is a *data item*). The client component[3] is an

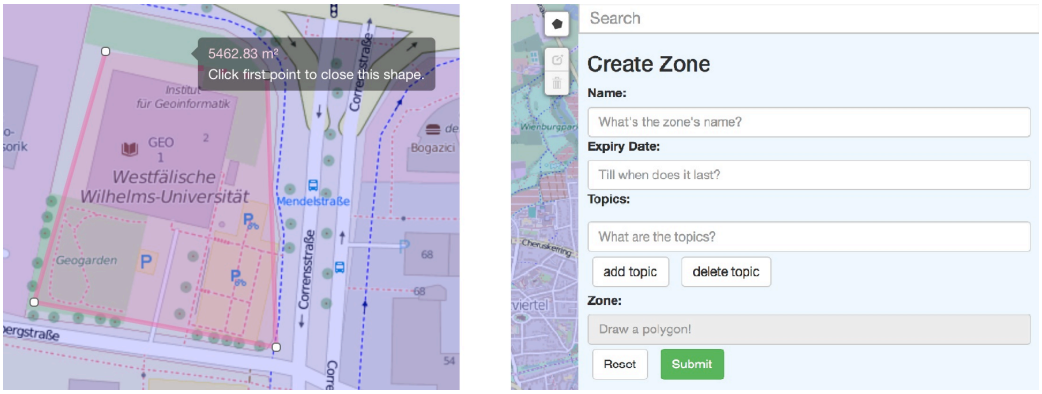


Fig. 5.1: Defining spatial zones in Happy Share (server component) by first drawing the boundary on the zone on a map (left) and then entering a name, expiration time and topic (right).

Android application the enables users to send and receive messages. It provides means to inspect and select available zones, to create messages, and to retrieve existing messages within a specific zone. Figure 5.2 shows several screenshots from the application. The user can select and show existing zones on a map. When the app opens, the user has to select one zone in which she wishes to operate and communicate (if she is physically in more than one zone). If she is in only one zone, this zone is automatically chosen, and the user can see the text "You are currently in [Zone]". A zone may have several topics, and the next step for the user is to select one (or many) topics of interest. For all topics selected, the user gets notified of new incoming messages related to the topic. She also has the possibility to see all messages related to a specific topic (e.g., Pokémon Go) with their respective expiration times. She can write messages related to one topic, and visualise (on a map) all past messages generated in the current zone she is in. While the system provides a full-featured location-based service – spatial messaging – it does so based on the concept of ephemerality. Two key features enable ephemerality in our prototype. The first one is the ability to specify an expiry time for every message, which effectively realises temporal ephemerality at the data level (a message is a *data item*). The second one is the ability to send a message only within a zone, i.e. a spatially well-defined and constrained area. Thereby, the concept of spatial ephemerality is realised. Both aspects do not only exist at the architectural or system level but are

[2] See `https://github.com/geo-c/sc16-ephemeral-lbs-server`.
[3] See `https://github.com/geo-c/SC-App`.

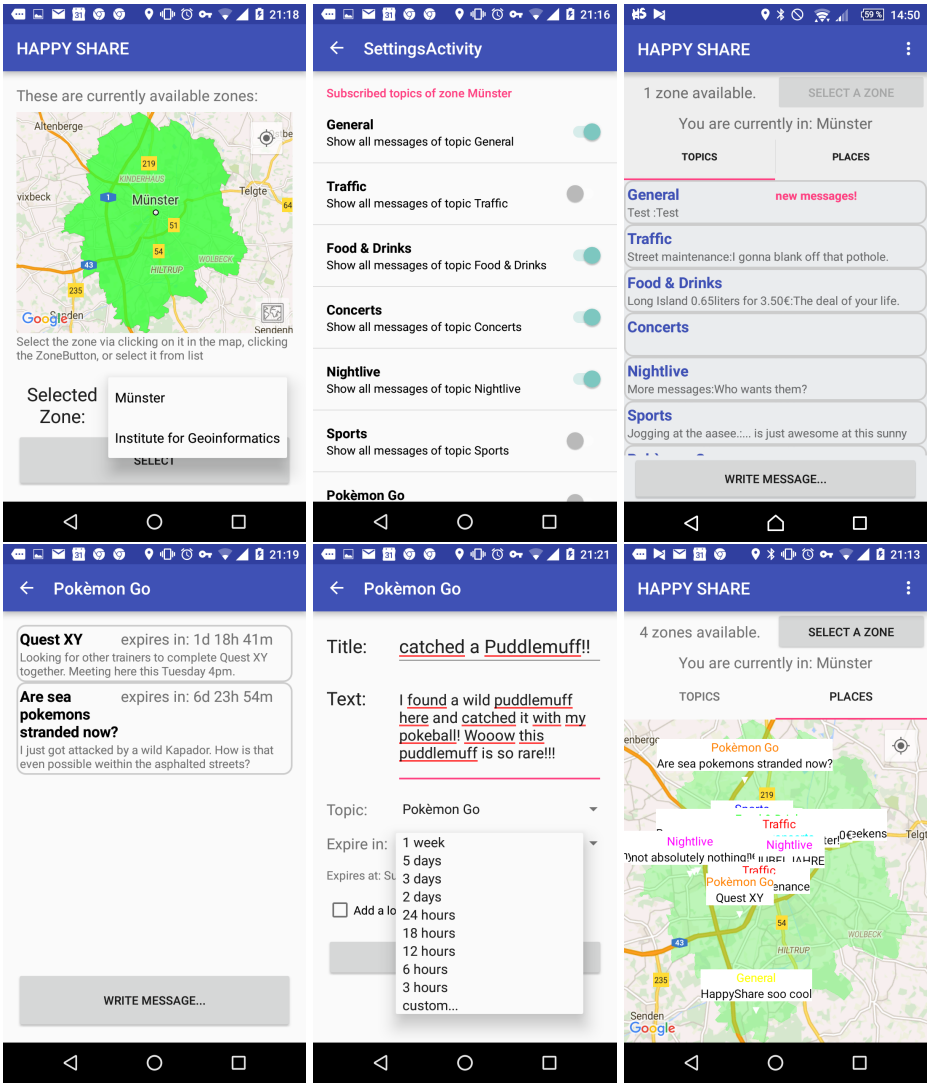


Fig. 5.2: Sending and receiving messages with the Happy Share client App. The user selects a spatial zone (top left), specifies topics of interest (top middle), receives notification about a new message for a topic (top right), visualizes existing messages for the “Pokémon Go" topic (bottom left), writes a message (bottom middle), and visualizes all messages within a spatial zone (bottom right).

also fully configurable at the interface level (see Figure 5.2). The UI elements for sending and retrieving messages within a specific zone are only accessible while the user resides inside the corresponding area. Users can also explicitly configure which zone a message is sent to (in case of overlapping regions) and how long their messages should persist before they are deleted. Overall, the prototype demonstrates that it is possible to develop a full-featured location-based service while at the same time implementing spatial and temporal ephemerality.

Regarding the storage of the data, the concept of ephemerality was introduced as the core concept of the location privacy management component. Storing the location data for a limited period can increase privacy by reducing the possibility of the attacks on stored location data and also decrease the need for storage to hold

the collected location data. However, these benefits come with some drawbacks. While the technical requirements for adding such components to the architecture of LBS is not complicated, the current economic culture of many service providers is based on their high interest in collecting and storing as much data as possible due to its commercial value, either for monetisation now or in the future. Therefore, persuading service providers to give away the commercial value of the location data in order to protect the user's location privacy is challenging. Besides, it might be equally challenging to persuade users to added complexity to their interaction with services (e.g. adjust the privacy setting) in order to increase their data privacy.

5.2.2 A Model to Design UI for Location Privacy

The excuse of avoiding increased complexity is not an adequate reason to stop asking for data privacy protection. Therefore, Chapter 3 focused on addressing guiding question no.2 "*How should user interfaces of LBS be designed to provide users with means to make informed choices about their location privacy?*". While the answer was thoroughly covered in chapter 3, its connection to other approaches and its benefits and drawbacks will be discussed in the next paragraphs.

Chapter 3 has proposed one way of realising the LP UI component of chapter 2. It combined Westin (2003)'s individual privacy theory, with privacy by design principles developed by Cavoukian (2010), and Shneiderman (2010)'s golden rules of interface design, into one model. This model was used to design a set of UIs that provide controls to adjust location data sharing. The UI elements were evaluated (e.g. User's perception and UIs relevance) through a user study. The results of the study indicate that the proposed UI design for fine-grained control of location privacy settings was received positively by participants. This positive feedback provides some initial evidence that the proposed theoretical model used to create the UI may be useful to design user interfaces for location privacy with the potential of fulfilling users' expectations. To summarise the findings in the study conducted in chapter 3, it is essential to highlight the underlying trade-offs of configuring location privacy settings. On the one hand, the fine-grained controls we provided enabled participants to specify in detail how and with whom they wanted to share location information. They were also able to respond to potential privacy threats in a nuanced way. On the other hand, managing location privacy is undoubtedly more complicated than a simple 'on/off' switch via UI controls. It also seems that given the right incentives, people give up their location privacy willingly.

Regarding UI and privacy management, Cranor, Guduru, and Arjula (2006) stated: "user interface designers need to find ways to manage the complexity, educate users about privacy, or express privacy concepts using language they already understand, guide users through the process of expressing their privacy preferences, and offer various options that meet the needs of a diverse set of users". There

are thus many parameters at play, and even if the proposed UI was well received, the results highlight the need for more studies to look further into aspects such as different contexts or incentives. Also in order to assure the ecological validity of this approach, there is a need for further field studies over an extended period of time.

5.2.3 Privacy Regulation for Location Privacy

In current practices, many of the mentioned challenges in previous sections (e.g. providing information regarding the collected personal data about users) receive the least amount of attention during the development processes of LBS. However, this is changing by the presence of regulations such as GDPR (EU, 2016). GDPR values user's data privacy and requires service providers to respect that. External forces, particularly in the form of laws could be a promising way to assure that service providers and data collectors consider the protection of personal data of users and act towards such protection with practical means. Taking GDPR and its requirements as an example in this context makes it possible to conclude that the proposed concept of ephemerality and also UI elements in previous chapters are in line with GDPR's expectations. GDPR explicitly requires service providers to provide the options for the users to be able to delete their personal data when they desire. The ephemerality concept can be a simple example of how technical measures (i.e. adding a new component to the architecture of LBS) can meet the legal requirements of recently established regulations. Although this example presents the potential of such approach but knowing how to bridge the gap between a legal text and understandable technical requirements is still one of the major difficulties with general legal data establishments such as GDPR. Thus, this work addressed this issue in Chapter 4 by extracting key factors and developing guidelines to facilitate the process of complying with regulations. Chapter 4 has developed an example for answering the guiding question number 3. "*How to comply with privacy legislation while developing LBS?*"

Chapter 4 selected the General Data Protection Regulation (GDPR) and examined the challenges of its implementation to answer this guiding question. This work generated a set of guidelines from the review of the GDPR's legal text and the analysis of expert interviews. The proposed guidelines can help designers and developers in designing UIs which are in line with GDPR requirements. The analysis in chapter 4 helps to distinguish a few aspects that need to be addressed according to GDPR. This work extracted aspects from GDPR regarding the communication of (location) privacy management with end users. These could be addressed at the UI level.

The perspective of addressing privacy at different levels (i.e. technical or UI) connects to the approach presented in Chapter 2. Different components such as Location Privacy Management and Location Privacy UI engage privacy-preserving solutions in various levels to reduce the complexity of the issue of addressing privacy

as a whole. The same approach was used for simplifying the legal text and extracting understandable instructions that are meaningful and useful for developers and designers of LBS while developing a service, with the ultimate purpose of building privacy-aware services and become GDPR compliant.

It is important to mention that the result presented in chapter 4 is subject to several limitations. The most important one is arguably that the proposed guidelines cannot guarantee that the resulting services will comply with all aspects of GDPR. This is mainly due to the guidelines only covering a subset of the GDPR (those aspects that can be addressed at the UI level). The aspects that this work did not realise were related to the management of data at the architecture level (e.g. data minimisation or end to end security). To overcome these two mentioned limitations, further steps would require a second cycle analysis of the legal text to extract the presented factors regarding the protection of data privacy entirely. In order to formulate a simplified instruction to address each of the factors in a practical way, there will be a need for exploring them with experts in software development and privacy and security engineers as well as advocates.

Given the complexity of the legislation and the topic in general, realising a comprehensive and consistent formal model of the GDPR appears to be a quite challenging task. There is a need for further research into areas such as practical ways of communicating privacy notices; user-friendly techniques of getting privacy consent, and genuinely enabling users control over their data. There is also a need to develop means for ensuring legal compliance, for instance to what extent service providers have to adjust their current technologies to reach the level of acceptable compliance.

5.3 Summary

A common connecting factor for the three presented approaches was to follow privacy by design principles by Cavoukian (2010) but also put an emphasis on developing practical solutions. The architecture (i.e. Subsec. 5.2.1) proposed an approach to manage location privacy. The model (i.e. Subsec. 5.2.2) developed for breaking down the complexity of the issue into three layers (i.e. Theory of privacy, privacy by design and, UI design rules). The guidelines (i.e. Subsec. 5.2.3) derived a set of instructions from the legal text of GDPR and expert interviews to help developers and designers to develop LBS that comply with GDPR. These approaches were applied to address the guiding questions.

The evaluation of the methods and solutions for protecting location privacy is one of the major challenges in the area. The number of practical tools specifically to measure and evaluate privacy are limited to a few like Westin privacy index (Kumaraguru and Cranor, 2005b) which makes it challenging to find a perfect tool

to evaluate and study (location) data privacy. One of the reasons for such difficulties is the fact that what users claim and do during a study is different from what they do in real life scenarios (D. Solove, 2008). This creates a discussion known as the *privacy paradox*, where users show concern regarding the protection of their privacy but their behaviour and attitudes are not inline with what they claim during the studies (Kokolakis, 2017).

When conducting user studies (e.g. interviews or evaluations), scientists face an ethical dilemma when trying to overcome the issue of the privacy paradox. On the one hand, by explaining to users that the study is about privacy, the result will suffer from bias. On the other hand, designing a deceptive study means an invasion of users privacy which has its own ethical implications. While this study also experienced some challenges regarding the evaluation of data privacy, the solutions for addressing those challenges were; to mix a number of methods, use an immersive environment to increase the realism of the scenarios, and (beside the use of standard user research methods i.e. interview and surveys) also develop prototypes and use cases to evaluate the usefulness and relevance of the proposed ideas through the use of final developed products. Due to ethical considerations, for the studies conducted in this thesis, the decision was to avoid any deception.

When discussing the benefits and drawbacks of addressing location data privacy, one needs to point out the underlying trade-offs of increased location privacy. On the one hand, the location privacy protection can increase, but users might face some difficulties in their interaction (e.g. adjusting the setting is complicated) or even miss a few functionalities (e.g. restricted location sharing can influence the accuracy of a navigation service). On the other hand, the loss of location privacy can have a negative impact on individuals lives (e.g. surveillance) or cause them damages like burglaries or stalking.

Furthermore, as a final reflection, in the context of protecting location data privacy, there is a need to create an eco-system of trust and transparency. Meaning that involved parties (e.g. hardware producers, service providers, developers, end users) should actively work towards building services that support transparency and trust. This will require practical changes in their current practices towards the development of LBS. For example, service providers and data controllers could present the relevant information regarding data privacy to users in a non-technical way, like, what kind of data is going to be collected, for what purposes, and who is going to have access to it. They could also include the explanation of the consequences of users' choices and the level of the trade-off linked to their decisions. The combination of such changes will promote a fair degree of transparency, and data privacy protection. The majority of this thesis focused on the role of developers and designers of LBS as responsible actors for assuring the design of privacy-aware services. However, in this context, it is crucial to mention that all involved parties are accountable and have the power to act and take practical steps towards building privacy-aware LBS.

6 Conclusion

> *Now, you and I both know that if you can control the flow of information, you can control everything.*
>
> — **Dave Eggers**
> (The Circle)

This thesis is about considering, managing and integrating location privacy while developing LBS. The first step in this context is to define relevant requirements regarding the protection of location privacy (e.g. the goal of the service or what location privacy means in that context). While the importance of protecting location privacy was discussed and demonstrated in previous chapters, the conclusion is that negotiating the expectations of different stakeholders is required in order to address privacy-related issues depending on each service's characteristics and goals (e.g. which data must be collected, for how long it should be stored and with whom is necessarily needs to be shared). Taking into account the three essential factors of the main research question (i.e. consideration, management and integration of location privacy), this work has addressed location privacy in the context of LBS architecture in chapter 2, UI design for LBS in chapter 3 and data privacy-related legalisation in chapter 4. The main contributions of this thesis are:

- **LBS architecture with privacy-preserving features:**
  In order to address privacy threats associated with the storage of location information, this work proposes an approach based on privacy-by-design principles and introduce a conceptual model to facilitate the implementation of those principles. In addition, this work investigates the role of location data management in the context of privacy preservation and proposes the concept of temporal and spatial ephemerality to improve location privacy in the context of a location-based service.

- **UI design for a fine-grained location privacy adjustment:**
  This work has provided a set of UI elements, grounded in existing privacy theories that facilitate fine-grained control of how location information is shared. These features inform users about what is happening to their location

data and then enable them to specify whom to share location with, when to share it, and where to share it. The exploratory study which evaluated the UI resulted in gathering insights into users' expectations regarding location privacy controls.

- **Guidelines to help developers to comply with aspects of GDPR that are addressable at UI level:**
  This work systematically analysed the legal text to identify aspects that can be or have to be addressed at the UI level for facilitating the protection of location data privacy. In addition, interviews with experts was carried out to gain further insights into the challenges arising from having to comply with the GDPR as well as into ways how and when to address them. Based on the outcome of both activities, the guidelines were developed for LBS developers and designers which could help them to design GDPR compliant services.

While both the technical and user-related aspects of a location-based service are essential for considering, managing and integrating location privacy, it is equally important to value the role of data privacy legislation in this process. Legal obligations are particularly useful for the cases when some service providers or data controllers prioritise their benefits over protecting users privacy. While such approaches are beneficial, this study learned that it is challenging to extract practical means from abstract principles to improve data privacy. Taking the privacy legalisation as an example, the complexity can increase when one realises that full compliance with data privacy regulations requires unique strategy development for each company or even each product. Constructing such unique strategies needs long-term collaboration among various parties such as service providers, developers, designers, system managers, data ethics activities, and legal specialists.

The overall conclusion is that initial consideration of (location) data privacy while deciding about the service architecture and its behaviour (i.e. what data to collect, how to store it and for how long) can play an exceptional role in building a privacy-aware service in the first place. Providing fine-grained controls for the users of LBS can also increase transparency which will eventually lead to increased acceptance of such services by users. Providing user-friendly privacy adjustment options can play a significant role in conveying to users the importance of location information protection. These factors are crucial while designing privacy protected services. As a final reflection on studies conducted in this thesis, it is possible to conclude that location privacy is an important issue which should be addressed by developers of LBS if they are hoping to build services that 1) are going to be accepted by users who have location privacy concerns, 2) users are going to be provided with an understanding of what happens with their location data, and 3) are going to comply with current data protection regulations.

6.1 Future research

Further work is needed in order to explore how to increase the awareness of the users of LBS regarding effective techniques to protect their (location) data privacy and also how to make them informed about the consequences of various decision makings with respect to data sharing practices. There is also a need for further studies on the possibilities of standardising UI design which can particularly be used to improve data privacy. In addition to such UI, it is needed to develop strategies for extracting practical instructions from legal and abstract privacy-related content in a systematic and organised way (e.g. the development of design patterns for privacy-related issues). It is also necessary to explore suitable educational strategies for service providers and data controllers with the goal of teaching them the consequences of their action regarding the personal data collection. There is, in general, a strong need for further work that supports the development of location-based services that are also location-privacy aware.

Bibliography

Abbas, Roba, Katina Michael, and MG Michael (2015). „Using a social-ethical framework to evaluate location-based services in an internet of things world“. In: *International Review of Information Ethics* 22.12, pp. 42–73 (cit. on pp. 1, 2, 15, 28).

Altman, Micah, Alexandra Wood, David R O'Brien, and Urs Gasser (2018). „Practical approaches to big data privacy over time“. In: *International Data Privacy Law* (cit. on pp. 95, 96).

Assad, Mark, David Carmichael, Judy Kay, and Bob Kummerfeld (2007). „Giving users control over location privacy“. In: *Fifth Workshop on Privacy in UbiComp*. Innsbruck, Austria (cit. on pp. 38, 54).

Ataei, Mehrnaz, Auriol Degbelo, and Christian Kray (2018). „Privacy theory in practice: designing a user interface for managing location privacy on mobile devices“. In: *Journal of Location Based Services*. in press (cit. on p. 64).

Ataei, Mehrnaz and Christian Kray (2017). „Ephemerality Is the New Black: A Novel Perspective on Location Data Management and Location Privacy in LBS“. In: pp. 357–373 (cit. on pp. 28, 36, 56).

Balogun, Adedayo M and Shao Ying Zhu (2013). „Privacy impacts of data encryption on the efficiency of digital forensics technology“. In: *arXiv preprint arXiv:1312.3183* (cit. on p. 15).

Bangor, Aaron, Philip Kortum, and James Miller (2009). „Determining what individual SUS scores mean: Adding an adjective rating scale“. In: *Journal of usability studies* 4.3, pp. 114–123 (cit. on p. 85).

Bargiotti, Leda, Inge Gielis, Bram Verdegem, et al. (2016). *Guidelines for public administrations on location privacy: European Union Location Framework*. Tech. rep. Joint Research Centre (Seville site) (cit. on p. 28).

Barkhuus, Louise and Anind K Dey (2003). „Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns.“ In: *Interact*. Vol. 3. Citeseer, pp. 702–712 (cit. on p. 12).

Benisch, Michael, Patrick Gage Kelley, Norman Sadeh, and Lorrie Faith Cranor (2011). „Capturing location-privacy preferences: Quantifying accuracy and user-burden tradeoffs“. In: *Personal and Ubiquitous Computing* 15.7, pp. 679–694 (cit. on pp. 31, 54).

Beresford, Alastair R and Frank Stajano (2003). „Location privacy in pervasive computing“. In: *IEEE Pervasive computing* 2.1, pp. 46–55 (cit. on pp. 2, 14, 16, 18, 64).

Beresford, Alastair R and Frank Stajano (2004). „Mix zones: User privacy in location-aware services“. In: *Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on*. IEEE, pp. 127–131 (cit. on p. 28).

Brandeis, Louis and Samuel Warren (1890). „The right to privacy“. In: *Harvard law review* 4.5, pp. 193–220 (cit. on pp. 6, 14).

Brooke, John et al. (1996). „SUS-A quick and dirty usability scale“. In: *Usability evaluation in industry* 189.194, pp. 4–7 (cit. on p. 85).

Brooke, John (2013). „SUS: A Retrospective“. In: *Journal of Usability Studies* 8.2, pp. 29–40 (cit. on p. 82).

Brush, A.J. Bernheim, John Krumm, and James Scott (2010). „Exploring End User Preferences for Location Obfuscation, Location-based Services, and the Value of Location“. In: *Proceedings of the 12th ACM International Conference on Ubiquitous Computing*. UbiComp '10. New York, NY, USA: ACM, pp. 95–104 (cit. on p. 28).

Budde, Reinhard, Karlheinz Kautz, Karin Kuhlenkamp, and Heinz Züllighoven (1992). „Prototyping“. In: *Prototyping*. Springer, pp. 33–46 (cit. on p. 7).

Cavoukian, Ann (2009). „Privacy by design“. In: *Take the challenge. Information and privacy commissioner of Ontario, Canada* (cit. on pp. 64, 65, 80, 87).

– (2010). „Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph. D“. In: *Identity in the Information Society* 3.2, pp. 247–251 (cit. on pp. 12, 16, 22, 33, 35, 39, 100, 102).

Chanchary, Farah and Sonia Chiasson (2015). „User perceptions of sharing, advertising, and tracking“. In: *Symposium on Usable Privacy and Security (SOUPS) 2015*. Ottawa, Canada: USENIX Association, pp. 53–67 (cit. on p. 30).

Chin, Erika, Adrienne Porter Felt, Vyas Sekar, and David Wagner (2012). „Measuring user confidence in smartphone security and privacy“. In: *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*. Washington, DC, USA: ACM Press, p. 1 (cit. on pp. 30, 31).

Chow, Chi-Yin and Mohamed F Mokbel (2009). „Privacy in location-based services: a system architecture perspective“. In: *Sigspatial Special* 1.2, pp. 23–27 (cit. on p. 13).

Church, Karen, Joachim Neumann, Mauro Cherubini, and Nuria Oliver (2010). „The map trap? An evaluation of map versus text-based interfaces for location-based mobile search services“. In: *Proceedings of the 19th International Conference on World Wide Web*. Raleigh, North Carolina, USA, pp. 261–270 (cit. on p. 32).

Claburn, Thomas (2017). *Wait, did Oracle tip off world to Google's creepy always-on location tracking in Android?* (Cit. on p. 38).

Clarke, Roger (1988). „Information technology and dataveillance“. In: *Communications of the ACM* 31.5, pp. 498–512 (cit. on pp. 2, 15, 28).

Clarke, Roger and Marcus Wigan (2011). „You are where you've been: the privacy implications of location and tracking technologies“. In: *Journal of Location Based Services* 5.3-4, pp. 138–155 (cit. on pp. 15, 28, 60).

Conger, Sue, Joanne H. Pratt, and Karen D. Loch (2013). „Personal information privacy and emerging technologies“. In: *Information Systems Journal* 23.5, pp. 401–417 (cit. on pp. 70, 71).

Consolvo, Sunny, Ian E Smith, Tara Matthews, et al. (2005). „Location disclosure to social relations: why, when, & what people want to share“. In: *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '05*. Ed. by Gerrit C. van der Veer and Carolyn Gale. Portland, Oregon, USA: ACM Press, p. 81 (cit. on pp. 31, 54).

Council, National Research et al. (2007). *Engaging privacy and information technology in a digital age*. National Academies Press (cit. on p. 14).

Cranor, Lorrie Faith, Praveen Guduru, and Manjula Arjula (2006). „User interfaces for privacy agents“. In: *ACM Transactions on Computer-Human Interaction (TOCHI)* 13.2, pp. 135–178 (cit. on p. 55).

Danculovic, Juan, Gustavo Rossi, Daniel Schwabe, and Leonardo Miaton (2001). „Patterns for personalized web applications“. In: *Proceedings of the 6th European Conference on Pattern Languages of Programms (EuroPLoP '2001)*. Ed. by Andreas Rüping, Jutta Eckstein, and Christa Schwanninger. Irsee, Germany: UVK - Universitaetsverlag Konstanz, pp. 423–436 (cit. on p. 63).

Delikostidis, Ioannis, Holger Fritze, Thore Fechner, and Christian Kray (2015). „Bridging the gap between field-and lab-based user studies for location-based services“. In: *Progress in Location-Based Services 2014*. Springer, pp. 257–271 (cit. on pp. 40, 41, 56).

Döweling, Sebastian, Benedikt Schmidt, and Andreas Göb (2012). „A model for the design of interactive systems based on activity theory“. In: *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work - CSCW '12*. Ed. by Steven E. Poltrock, Carla Simone, Jonathan Grudin, Gloria Mark, and John Riedl. Seattle, Washington, USA: ACM Press, pp. 539–548 (cit. on p. 87).

Duckham, Matt and Lars Kulik (2006). „Location privacy and location-aware computing“. In: *Dynamic & mobile GIS: investigating change in space and time* 3, pp. 35–51 (cit. on pp. 3, 14, 15, 28, 62, 84).

Eggers, Dave (2015). *The circle*. Art People (cit. on p. 96).

Epstein, Daniel A, Alan Borning, and James Fogarty (2013). „Fine-grained sharing of sensed physical activity: a value sensitive approach“. In: *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing*. ACM, pp. 489–498 (cit. on p. 32).

EU (2016). *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). A subtitle (optional)* (cit. on pp. 4, 60, 63, 65–68, 70, 75, 77, 78, 90, 91, 96, 101).

Fawaz, Kassem, Huan Feng, and Kang G Shin (2015). „Anatomization and protection of mobile apps' location privacy threats“. In: *24th USENIX Security Symposium (USENIX Security 15)*. Washington, DC, USA: USENIX Association, pp. 753–768 (cit. on pp. 29, 62).

Fawaz, Kassem and Kang G Shin (2014). „Location privacy protection for smartphone users“. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14*. Ed. by Gail-Joon Ahn, Moti Yung, and Ninghui Li. Scottsdale, Arizona, USA: ACM Press, pp. 239–250 (cit. on p. 28).

Felt, Adrienne Porter, Serge Egelman, and David Wagner (2012). „I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns". In: *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, pp. 33–44 (cit. on p. 2).

Fodor, Mark and Alexander Brem (2015). „Do privacy concerns matter for Millennials? Results from an empirical analysis of Location-Based Services adoption in Germany". In: *Computers in Human Behavior* 53, pp. 344–353 (cit. on pp. 2, 12).

Gartner, Georg (2004). „Location-based mobile pedestrian navigation services – the role of multimedia cartography". In: *Joint Workshop on Ubiquitous, Pervasive and Internet Mapping (UPIMap2004)*. Tokyo, Japan (cit. on p. 32).

Hightower, Jeffrey, Barry Brumitt, and Gaetano Borriello (2002). „The location stack: A layered model for location in ubiquitous computing". In: *Mobile Computing Systems and Applications, 2002. Proceedings Fourth IEEE Workshop on*. IEEE, pp. 22–28 (cit. on pp. 13, 18).

Hoh, Baik, Marco Gruteser, Hui Xiong, and Ansaf Alrabady (2006). „Enhancing security and privacy in traffic-monitoring systems". In: *IEEE Pervasive Computing* 5.4, pp. 38–46 (cit. on pp. 2, 15).

Hornbæk, Kasper and Antti Oulasvirta (2017). „What is interaction?" In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*. Ed. by Gloria Mark, Susan R. Fussell, Cliff Lampe, et al. Denver, Colorado, USA: ACM Press, pp. 5040–5052 (cit. on p. 70).

Hsieh, Hsiu-Fang and Sarah E. Shannon (2005). „Three approaches to qualitative content analysis". In: *Qualitative Health Research* 15.9, pp. 1277–1288 (cit. on p. 72).

Iachello, Giovanni, Ian Smith, Sunny Consolvo, Mike Chen, and Gregory D. Abowd (2005). „Developing privacy guidelines for social location disclosure applications and services". In: *Proceedings of the 2005 Symposium on Usable Privacy and Security*. Ed. by Lorrie Faith Cranor. Pittsburgh, Pennsylvania, USA: ACM Press, pp. 65–76 (cit. on p. 33).

Ivory, Melody Y and Marti A Hearst (2001). „The state of the art in automating usability evaluation of user interfaces". In: *ACM Computing Surveys (CSUR)* 33.4, pp. 470–516 (cit. on p. 87).

Junglas, Iris A and Richard T Watson (2008). „Location-based services". In: *Communications of the ACM* 51.3, pp. 65–69 (cit. on pp. 1, 12).

Kang, Ruogu, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler (2015). „"My data just goes everywhere": User mental models of the internet and implications for privacy and security". In: *Symposium on Usable Privacy and Security (SOUPS) 2015*. Ottawa, Canada: USENIX Association, pp. 39–52 (cit. on p. 30).

Keßler, Carsten and Grant McKenzie (2018). „A geoprivacy manifesto". In: *Transactions in GIS* 22.1, pp. 3–19 (cit. on pp. 6, 15, 62, 64, 96).

Kido, Hidetoshi, Yutaka Yanagisawa, and Tetsuji Satoh (2005). „An anonymous communication technique using dummies for location-based services". In: *Pervasive Services, 2005. ICPS'05. Proceedings. International Conference on*. IEEE, pp. 88–97 (cit. on p. 13).

Kobsa, Alfred (2007). „Privacy-enhanced personalization". In: *Communications of the ACM* 50.8, pp. 24–33 (cit. on pp. 63, 64).

Kokolakis, Spyros (2017). „Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon“. In: *Computers & Security* 64, pp. 122–134 (cit. on p. 103).

Korff, Stefan and Rainer Böhme (2014). „Too much choice: end-user privacy decisions in the context of choice proliferation“. In: *Tenth Symposium on Usable Privacy and Security, SOUPS 2014*. Ed. by Lorrie Faith Cranor, Lujo Bauer, and Robert Biddle. Menlo Park, California, USA: USENIX Association, pp. 69–87 (cit. on p. 31).

Krumm, John (2007). „Inference attacks on location tracks“. In: *International Conference on Pervasive Computing*. Springer, pp. 127–143 (cit. on p. 16).

– (2009). „A survey of computational location privacy“. In: *Personal and Ubiquitous Computing* 13.6, pp. 391–399 (cit. on pp. 1, 2, 12, 15, 16, 28, 35, 60).

Kumaraguru, Ponnurangam and Lorrie Faith Cranor (2005a). *Privacy indexes: A survey of westin's studies*. Tech. rep. December, pp. 1–22 (cit. on p. 30).

– (2005b). *Privacy indexes: a survey of Westin's studies*. Carnegie Mellon University, School of Computer Science, Institute for Software Research International (cit. on p. 102).

Langheinrich, Marc (2002). „A privacy awareness system for ubiquitous computing environments“. In: *international conference on Ubiquitous Computing*. Springer, pp. 237–245 (cit. on pp. 28, 64).

Lazar, Jonathan, Jinjuan Heidi Feng, and Harry Hochheiser (2017). *Research methods in human-computer interaction*. Morgan Kaufmann (cit. on p. 7).

Leda Bargiotti, Inge Gielis, Bram Verdegem, Pieter Breyne, Francesco Pignatelli, Paul Smits Ray Boguslawski (2016). *Guidelines for public administrations on location privacy. A subtitle (optional)* (cit. on p. 74).

Ledo, David, Steven Houben, Jo Vermeulen, et al. (2018). „Evaluation strategies for HCI toolkit research“. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*. Ed. by Regan L. Mandryk, Mark Hancock, Mark Perry, and Anna L. Cox. Montreal, Quebec, Canada: ACM Press, pp. 1–17 (cit. on p. 82).

Lee, Dik Lun, Manli Zhu, and Haibo Hu (2005). „When location-based services meet databases“. In: *Mobile Information Systems* 1.2, pp. 81–90 (cit. on p. 17).

Lewis, James R and Jeff Sauro (2009). „The factor structure of the system usability scale“. In: *International conference on human centered design*. Springer, pp. 94–103 (cit. on p. 85).

Lin, Jialiu, Michael Benisch, Norman Sadeh, et al. (2013). „A comparative study of location-sharing privacy preferences in the United States and China“. In: *Personal and Ubiquitous Computing* 17.4, pp. 697–711 (cit. on p. 54).

Lin, Jialiu, Bin Liu, Norman Sadeh, and Jason I. Hong (2014). „Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings“. In: *Tenth Symposium on Usable Privacy and Security, SOUPS 2014*. Ed. by Lorrie Faith Cranor, Lujo Bauer, and Robert Biddle. Menlo Park, California, USA: USENIX Association, pp. 199–212 (cit. on pp. 30, 56).

Lin, Yu-Wei (2018). „# DeleteFacebook is still feeding the beast–but there are ways to overcome surveillance capitalism“. In: *The Conversation* (cit. on p. 60).

Loomis, Jack M, James J Blascovich, and Andrew C Beall (1999). „Immersive virtual environment technology as a basic research tool in psychology“. In: *Behavior Research Methods, Instruments, & Computers* 31.4, pp. 557–564 (cit. on p. 41).

Malaka, Rainer and Alexander Zipf (2000). „Deep Map: Challenging IT research in the framework of a tourist information system“. In: *Information and communication technologies in tourism 2000*. Springer, pp. 15–27 (cit. on p. 13).

Margulis, Stephen T (2003). „On the status and contribution of Westin's and Altman's theories of privacy“. In: *Journal of Social Issues* 59.2, pp. 411–429 (cit. on p. 35).

Margulis, Stephen T. (2011). *Three theories of privacy: An overview*. Ed. by Sabine Trepe and Leonard Reinecke. Springer-Verlag (cit. on p. 34).

McKenzie, Grant, Krzysztof Janowicz, and Dara Seidl (2016). „Geo-privacy beyond coordinates“. In: *Geospatial Data in a Changing World - Selected papers of the 19th AGILE Conference on Geographic Information Science*. Ed. by T Sarjakoski, Maribel Yasmina Santos, and L. Tiina Sarjakoski. Helsinki, Finland: Springer International Publishing, pp. 157–175 (cit. on p. 62).

Medicare & Medicaid Services, Centers for et al. (2008). „Selecting a development approach“. In: *Centers for Medicare & Medicaid Services*, pp. 1–10 (cit. on p. 80).

Michael, Katina and MG Michael (2011). *The social and behavioural implications of location-based services* (cit. on p. 2).

Mokbel, Mohamed F, Chi-Yin Chow, and Walid G Aref (2006). „The new casper: Query processing for location services without compromising privacy“. In: *Proceedings of the 32nd international conference on Very large data bases*. VLDB Endowment, pp. 763–774 (cit. on pp. 16, 18, 19, 64).

Mokbel, Mohamed F., Thanaa M. Ghanem, and Walid G. Aref (2003). „Spatio-temporal access methods“. In: *IEEE Data Eng. Bull.* 26.2, pp. 40–49 (cit. on p. 18).

Narayanan, Arvind, Narendran Thiagarajan, Mugdha Lakhani, Michael Hamburg, Dan Boneh, et al. (2011). „Location Privacy via Private Proximity Testing.“ In: *NDSS*. Vol. 11 (cit. on p. 31).

Newman, A. L. (2015). „What the "right to be forgotten" means for privacy in a digital age“. In: *Science* 347.6221, pp. 507–508 (cit. on p. 60).

O'Hara, Kenton (2008). „Understanding geocaching practices and motivations“. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, pp. 1177–1186 (cit. on p. 12).

Olsen, Dan R. (2007). „Evaluating user interface systems research“. In: *Proceedings of the 20th annual ACM symposium on User interface software and technology - UIST '07*. Ed. by Chia Shen, Robert J. K. Jacob, and Ravin Balakrishnan. Newport, Rhode Island, USA: ACM Press, pp. 251–258 (cit. on p. 81).

Olumofin, Femi, Piotr K Tysowski, Ian Goldberg, and Urs Hengartner (2010). „Achieving efficient query privacy for location based services“. In: *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, pp. 93–110 (cit. on p. 31).

Patil, Sameer, Greg Norcie, Apu Kapadia, and Adam J Lee (2012). „Reasons, rewards, regrets: Privacy considerations in location sharing as an interactive practice“. In: *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*. Ed. by Lorrie Faith Cranor. Washington, DC, USA: ACM Press, p. 1 (cit. on pp. 31, 47).

Patterson, Donald J, Lin Liao, Dieter Fox, and Henry Kautz (2003). „Inferring high-level behavior from low-level sensors“. In: *International Conference on Ubiquitous Computing*. Springer, pp. 73–89 (cit. on pp. 2, 15).

Pfitzmann, Andreas and Marit Hansen (2010). „A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management“. In: (cit. on p. 35).

Ran, Lisa, Sumi Helal, and Steve Moore (2004). „Drishti: an integrated indoor/outdoor blind navigation system and service“. In: *Pervasive Computing and Communications, 2004. PerCom 2004. Proceedings of the Second IEEE Annual Conference on*. IEEE, pp. 23–30 (cit. on p. 12).

Raschke, Philip, Axel Küpper, Olha Drozd, and Sabrina Kirrane (2017). „Designing a GDPR-Compliant and Usable Privacy Dashboard“. In: *IFIP International Summer School on Privacy and Identity Management*. Springer, pp. 221–236 (cit. on p. 96).

Rinner, C, M Raubal, and B Spigel (2005). „User interface design for location-based decision services“. In: *13th International Conference on GeoInformatics*. Citeseer, pp. 17–19 (cit. on p. 31).

Sathe, Saket, Roie Melamed, Peter Bak, and Shivkumar Kalyanaraman (2014). „Enabling Location-Based Services 2.0: Challenges and Opportunities“. In: *Mobile Data Management (MDM), 2014 IEEE 15th International Conference on*. Vol. 1. IEEE, pp. 317–320 (cit. on p. 17).

Schaub, Florian, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor (2015). „A design space for effective privacy notices“. In: *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pp. 1–17 (cit. on pp. 33, 87).

Schaub, Florian, Bastian Könings, and Michael Weber (2015). „Context-adaptive privacy: Leveraging context awareness to support privacy decision making“. In: *IEEE Pervasive Computing* 14.1, pp. 34–43 (cit. on p. 2).

Schiller, Jochen (2004). *A., Voisard: Location-Based Services* (cit. on pp. 13, 18).

Schmitz Weiss, Amy (2013). „Exploring news apps and location-based services on the smartphone“. In: *Journalism & Mass Communication Quarterly* 90.3, pp. 435–456 (cit. on p. 1).

Scipioni, Marcello Paolo and Marc Langheinrich (2011). „Towards a New Privacy-Aware Location Sharing Platform.“ In: *J. Internet Serv. Inf. Secur.* 1.4, pp. 47–59 (cit. on p. 54).

Shneiderman, Ben (2010). *Designing the user interface: strategies for effective human-computer interaction*. Pearson Education India (cit. on pp. 33, 36, 39, 100).

Solove, Daniel (2008). „Understanding privacy“. In: (cit. on pp. 6, 61, 103).

Solove, Daniel J (2002). „Conceptualizing privacy“. In: *Cal. L. Rev.* 90, p. 1087 (cit. on p. 62).

– (2005). „A taxonomy of privacy“. In: *U. Pa. L. Rev.* 154, p. 477 (cit. on pp. 6, 29).

Spiekermann, Sarah (2004). „General Aspects of“. In: *Location-based services* 9, pp. 14–33 (cit. on p. 13).

Steiniger, Stefan, Moritz Neun, Alistair Edwardes, and Barbara Lenz (2008). „Foundations of LBS“. In: *CartouCHe-Cartography for Swiss Higher Education. Obtido em* 20, p. 2010 (cit. on p. 13).

Stroeken, K, A Verdoolaege, M Versichele, et al. (2015). „Zone-it before IT zones you: a location-based digital notice board to build community while preserving privacy“. In: *Journal of Location Based Services* 9.1, pp. 16–32 (cit. on pp. 15, 16, 32, 54).

Sun, Xu and Andrew May (2013). „A comparison of field-based and lab-based experiments to evaluate user experience of personalised mobile devices“. In: *Advances in Human-Computer Interaction* 2013, pp. 1–9 (cit. on p. 40).

Sweeney, Latanya (2002). „k-anonymity: A model for protecting privacy“. In: *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10.05, pp. 557–570 (cit. on pp. 20, 64).

Toch, Eran, Justin Cranshaw, Paul Hankes Drielsma, et al. (2010). „Empirical models of privacy in location sharing“. In: *Proceedings of the 12th ACM International Conference on Ubiquitous Computing - Ubicomp '10*. Ed. by Jakob E. Bardram, Marc Langheinrich, Khai N. Truong, and Paddy Nixon. April 2016. Copenhagen, Denmark: ACM Press, p. 129 (cit. on pp. 20, 32, 38).

Tsai, Janice Y, Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh (2010). „Location-sharing technologies : Privacy risks and controls“. In: *A Journal of Law and Policy for the Information Society* 6.2, pp. 119–151 (cit. on p. 38).

Tsai, Janice Y, Patrick Kelley, Paul Drielsma, et al. (2009). „Who's viewed you? The impact of feedback in a mobile location-sharing application“. In: *Proceedings of the 27th international conference on Human factors in computing systems - CHI 09*. Ed. by Dan R. Olsen Jr., Richard B. Arthur, Ken Hinckley, et al. Boston, Massachusetts, USA: ACM Press, pp. 2003–2012 (cit. on pp. 31, 53).

Wang, Edward Shih-Tse and Ruenn-Lien Lin (2017). „Perceived quality factors of location-based apps on trust, perceived privacy risk, and continuous usage intention“. In: *Behaviour & Information Technology* 36.1, pp. 2–10 (cit. on p. 4).

Ward, Steven, Kate Bridges, and Bill Chitty (2005). „Do incentives matter? An Examination of on-line privacy concerns and willingness to provide personal and financial information“. In: *Journal of Marketing Communications* 11.1, pp. 21–40 (cit. on p. 55).

Westin, Alan F. (2003). „Social and political dimensions of privacy“. In: *Journal of Social Issues* 59.2, pp. 431–453 (cit. on pp. 14, 33–35, 37, 38, 61, 100).

Xie, Jierui, Bart Piet Knijnenburg, and Hongxia Jin (2014). „Location sharing privacy preference: analysis and personalized recommendation“. In: *Proceedings of the 19th international conference on Intelligent User Interfaces*. Haifa, Israel: ACM Press, pp. 189–198 (cit. on p. 54).

Xu, Heng and Sumeet Gupta (2009). „The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services“. In: *Electronic Markets* 19.2-3, pp. 137–149 (cit. on p. 14).

Zakhary, Victor, Cetin Sahin, Theodore Georgiou, and Amr El Abbadi (2017). „LocBorg: Hiding social media user location while maintaining online persona (vision paper)“. In: *25th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (ACM SIGSPATIAL 2017)*. Los Angeles, California, USA: ACM Press (cit. on p. 28).

Zhou, Tao (2011). „The impact of privacy concern on user adoption of location-based services“. In: *Industrial Management & Data Systems* 111.2, pp. 212–226 (cit. on pp. 2, 14).

Websites

BIA/Kelsey (2016). *Location-Targeted Mobile Ad Spend to Reach $29.5B in the U.S.* URL: http://www.biakelsey.com/location-targeted-mobile-ad-spend-reach-29-5b-u-s-2020/ (visited on July 29, 2018) (cit. on p. 95).

Deeyfuss, Emily (2017). *BLAMING THE INTERNET FOR TERRORISM MISSES THE POINT*. URL: https://www.wired.com/2017/06/theresa-may-internet-terrorism/ (visited on July 20, 2018) (cit. on p. 96).

Economist, The (2017). *The world's most valuable resource is no longer oil, but data*. URL: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (visited on July 29, 2018) (cit. on p. 95).

Foursquare (2016a). URL: https://foursquare.com/ (visited on June 15, 2016) (cit. on p. 12).

– (2016b). URL: https://foursquare.com/ (visited on June 15, 2016) (cit. on p. 12).

Harding, luke (2015). *Mass surveillance is fundamental threat to human rights, says European report*. URL: https://www.theguardian.com/world/2015/jan/26/mass-surveillance-threat-human-rights-council-europe (visited on July 30, 2018) (cit. on p. 96).

Temming, Maria (2018). *Your phone is like a spy in your pocket*. URL: https://www.sciencenews.org/article/smartphones-data-collection-security-privacy (visited on July 29, 2018) (cit. on p. 96).

Tsukayama, Hayley (2018). *Don't want Google tracking you? You have almost no choice, according to a study*. URL: https://www.washingtonpost.com/technology/2018/08/22/dont-want-google-tracking-you-you-have-almost-no-choice-according-new-study/?noredirect=on&utm_term=.f0c7704fd196 (visited on Aug. 21, 2018) (cit. on p. 96).

List of Abbreviations

API	Application Program Interface
DPD	Data Protection Directive
EU	European Union
GPS	Global Positioning System
HCI	Human-Computer Interaction
LBS	Location-Based Services
LPM	location Privacy Management Component
LP UI	Location Privacy User Interface
NCC	Notice - Consent - Control
PET	Privacy-Enhancing Technologies
UI	User Interfaces
UX	User Experiences

MEHRNAZ ATAEI

Rudolf-Harbig Weg 2b | Münster | Germany
+49157 85459383 | m.ataei@uni-muenster.de

EDUCATION

2015-2018 **PhD candidate - Location Data Privacy**
Münster University
Germany

2010-2013 **Master of Science in Informatics - Human Computer Interaction**
Umeå University
Sweden

2003- 2008 **Bachelor of Science in Computer science - Software Engineering**
Kashan University
Iran

EXPERIENCE

2014-2015 **Interaction Designer**
LokkUpp
Sweden

2009-2010 **ICT Tutor**
Safir Institute
Iran

Mehrnaz Ataei
August 2018
Münster - Germany

Location Data Privacy : Principles to Practice

Location data is essential to the provision of relevant and tailored information in location-based services (LBS) but has the potential to reveal sensitive information about users. Unwanted disclosure of location data is associated with various threats known as *dataveillance* which can lead to risks like loss of control, (continuous) monitoring, identification, and social profiling. Striking a balance between providing a service based on the user's location while protecting their (location) privacy is thus a key challenge in this area. Although many solutions have been developed to mitigate the data privacy-related threats, the aspects involving users (i.e. User Interfaces (UI)) and the way in which location data management can affects (location) data privacy have not received much attention in the literature.

This thesis develops and evaluates approaches to facilitate the design and development of privacy-aware LBS. This work has explicitly focused on three areas: location data management in LBS, the design of UI for LBS, and compliance with (location) data privacy regulation. To address location data management, this thesis proposes modifications to LBS architectures and introduces the concept of temporal and spatial ephemerality as an alternative way to manage location privacy. The modifications include adding two components to the LBS architecture: one component dedicated to the management of decisions regarding collected location data such as applying restriction on the time that the service provider stores the data; and one component for adjusting location data privacy settings for the users of LBS. This thesis then develops a set of UI controls for fine-grained management of location privacy settings based on privacy theory (Westin), privacy by design principles and general UI design principles. Finally, this thesis brings forth a set of guidelines for the design and development of privacy-aware LBS through the analysis of the General Data Protection Regulation (GDPR) and expert recommendations.

Service providers, designers, and developers of LBS can benefit from the contributions of this work as the proposed architecture and UI model can help them to recognise and address privacy issues during the LBS development process. The developed guidelines, on the other hand, can be helpful when developers and designers face difficulties understanding (location) data privacy-related regulations. The guidelines include both a list of legal requirements derived from GDPR's text and expert suggestions for developers and designers of LBS in the process of complying with data privacy regulation.

WWU
MÜNSTER

2018