Privacy in Location-Based Services and Their Criticality Based on Usage Context

Tom Lorenz, Ina Schiering

Privacy in Location-Based Services and their Criticality based on Usage Context

Tom Lorenz, Ina Schiering

Ostfalia University of Applied Sciences
Wolfenbüttel, Germany
{tom.lorenz1, i.schiering}@ostfalia.de

Abstract. Location based services are an important trend for smart city services, mobility and navigation services, fitness apps and augmented reality applications. Because of the growing significance of location-based services, location privacy is an important aspect. Typical use cases are identified and investigated based on user perceptions of usefulness and intrusiveness. In addition criticality of services is evaluated taking the typical technical realization into account. In the context of this analysis the implication of privacy patterns is investigated. An overall criticality rating based on applied location privacy patterns is proposed and thoroughly discussed, while taking the decrease of usability into consideration.

Keywords: location-based services, smart city, location privacy, tracking, augmented reality, privacy risks

1 Introduction

The consideration of location and movement information is used by various location based services and smart city services. It was investigated especially in the context of ubiquitous computing as described by Bellavista et al. [2]. There are applications as navigation, tracking of children and pets, location-based mobile gaming, dating and fitness apps. Recent examples are games as Pokémon Go [31], the upcoming augmented reality-game "Harry Potter Wizards Unite" [1] and location based dating apps [14]. In the context of smart cities location data is used by public institutions for infrastructure and commerce planning [35]. Applications using location based information are frequently described as *Location Tracking* resp. *Location Awareness*. Also the notions *Participatory Sensing* and *Pervasive Location Awareness* are used [11].

Privacy risks concerning the usage of location based data and the concept of location privacy were investigated by Beresford et al. [3]. There location privacy is defined as "the ability to prevent other parties from learning one's current or past location". Finn et al. [13] define privacy of location and space as that "individuals have the right to move about in public or semi-public space without being identified, tracked or monitored". Location data is specified in the

[1] https://www.harrypotterwizardsunite.com/

General Data Protection Regulation (GDPR) Article 4(1) as one means of identification of natural persons. In Recital 75 the analysis or prediction of location or movement is considered as a privacy risk.

The aim of this paper is to investigate location privacy in specific usage contexts. To this aim use cases for typical location based services are described. Based on the analysis of privacy risks and privacy concerns in the context of location based services, a categorization for privacy risks is proposed considering criticality of use cases based on typical realizations and user perceptions of intrusiveness and usefulness. Afterwards the applicability of privacy patterns and the impact on the analysis is investigated.

2 Background

2.1 Indoor and Outdoor Localization

Smart devices offer various possibilities for generating location information. For outdoor localization and navigation the use of *Global Positioning System* (GPS) sensors is the approach mainly used. The position can be efficiently calculated based on trilateration (see Fig. 1(a)[2]) on a low-cost basis and necessary hardware is easily obtainable due to large-scale production.

(a) Trilateration achieved by satellites in the case of GPS

(b) relevant feature lines used in Visual Landmark Detection [6]

Fig. 1: Localization Methods

For indoor localization other approaches exist since satellite signals are hardly receivable due to modern building style. Even for low signal strengths, positioning is not reasonable since due to indoor environment even a couple of meters could mean a difference in offices or floors respecting vertical accuracy. Therefore some approaches rely on additional infrastructure in the environment. Beside

[2] Source: https://gisgeography.com/trilateration-triangulation-gps/

Near-Field Communication (NFC) and beacons also approaches based on 3D object detection as used for *Augmented Reality* (AR) devices as the Microsoft HoloLens [16] or behavior based approaches as proposed in [37] are used. Table 1 summarizes localization approaches.

Positioning algorithms using beacons or NFC work mainly similar to GPS based algorithms via trilateration (see Fig. 1(a)). For NFC based algorithms user devices may also include NFC reading technology and can therefore calculate their own position based on incoming signals [25]. Alternatively, users may have a fixed NFC tag used for identifying themselves on specific NFC Readers (e.g. used in public transport which could potentially also be used in location based games). Beacons or NFC Tags that are able to cover the needed building or area are required.

Other approaches use a device carried by the user itself. These behavior based approaches use multiple sensors like accelerometer, gyroscope or magnetometer to notice positional changes and obtain a position by mapping these changes and building hypotheses concerning the actual position. Often a combination of sensors is integrated in an *inertial measurement unit* (IMU). Due to the increasing number of smartphones and depending on the built in sensors of the device itself, this method is very flexible and cheap since a new area do not have to be equipped with beacons beforehand. Fitness trackers calculate the covered distance by a derived step size based on the body height. That this step size might change based on hurry or company is not taken into consideration in these distance estimations. In general, the results of these approaches are still not very robust.

	GPS	**Beacons**	**NFC**	**Visual**	**IMU**	**Hololens**
Indoor Localization	✗	✓	❍	❍	❍	✓
Outdoor Localization	✓	❍	✗	❍	❍	❍
HW costs	↓	↑	❍	↓	↓	↑
SW complexity	↓	↓	↓	↑	❍	↑
Cloud computation needed	✗	✗	✗	✓	❍	❍
Computation on device sufficient	✓	✓	✓	✗	❍	✗

Table 1: Analysis of Localization Approaches - yes (✓), depends / medium (❍), no (✗), high (↑), low (↓)

In addition to these sensor based approaches other localization methods use visual input for localization. One approach is to compute a positional change or motion based on the exact alteration of distinctive points in a video stream. This approach is called visual odometry [27,28]. Based on the use case visual odometry can come in quite handy since it is also viable with a single camera and can be calculated on the device if the video stream quality is reduced. It is also used by the NASA since it only relies on camera input [33].

Another viable approach are visual landmarks. Photos or outlines of distinctive environmental objects, e.g. buildings, sights or places can be used for a rough

localization by comparing the current photo to a subset of existing similar photos of given landmarks (see Fig. 1(b)). Due to the high number of comparisons and the corresponding high amount of computational power needed, this technique is mostly realized via cloud services [30,6]. Although perspective transformations are possible, a big dataset of distinctive objects is needed. These transformations allow for an image correction of small angles but information of buildings backsides or other points of views have to be covered in the data set as well. A 3D Model of the designated building might be viable as well. Mapping the current 3D area to a previously scanned three dimensional space is possible as well [18], but as soon as the environment exceeds an office, additional enhancements are needed. Further the HoloLens uses a combination of sensors, e.g. distance sensors and 3D mapping to distinguish its position. To speed up certain processes these areas are recognized and distinguished by a WiFi signal [20].

2.2 Privacy Patterns for Localization Information

Since specific locations e.g. homes are directly bound to a person, anonymized location data can often be successfully deanonymized. By composing several distinct data sets, also called linking, tracking of individuals is possible therefore resulting in deanonymization of the given location data as described in [24,8,5]. To reduce the risk of deanonymization, countermeasures in the form of privacy enhancing techniques (privacy patterns) are investigated in the context of the use cases described in Section 5.1. In the following privacy patterns for localization information are explained and summarized:

- **Discretized Points on Grid:** is a pattern that aligns current GPS positions on a predetermined grid. These calculations are done locally on the device before sending locational information to the service provider. Hence privacy is increased by decreasing accuracy [22].
- **Delays:** are introduced to add noise to the point in time of a position. Both small (couple of seconds) and big delays (couple of hours) are considered. While adding always a fixed amount is insufficient, a random amount of time is added to the original time stamp of the positional info or waited on the device before sending a request to the service provider. A higher limit allows for bigger time gaps and therefore increased privacy in contrast to small delays which, on the other hand side might not influence the usability as much.
- **Fixed Time Slots:** are similar to the described delays, but instead of adding a delay to the point in time of a given position, the positioning itself is only done every x minutes or hours. Mostly fixed time slots are more user-friendly since even if the waiting time of a delay might be shown to the user before each transmission, it is still randomized. Using a fixed time slot allows the user or service provider some kind of predictability when to expect the next update.
- **Dummy Users:** can be applied by adding Gaussian noise to the positional data. Therefore instead of sending just one position to the server, multiple

positions are sent. From the information received by the service the correct result can be filtered based on the current position of the user [22].This method leads to very accurate results for the user itself, but also results in higher data transfer and more processing on the device and also for the service provider, since many of these requested information are not used after receiving them on the device. Also this approach might not be suitable for use cases, where exact positions of the users might needed to provide information for a whole community. The process of generating realistic noise is not that trivial in certain cases as well.

Mix Zones are also a common method for achieving location privacy. While k-anonymity cannot be achieved by a single device alone, it furthermore relies on a user base being in the same area with permanent changing pseudonyms to ensure ongoing privacy [4]. Furthermore linkability is feasible if the distance between mix zones varies and users need different a amount of times to reach them. Anonymity or at least pseudonymity can be achieved easily by adding a specific layer between user and service provider [29]. But these approaches hold a similar problem. If not enough user are in a close area, a person is easily traceable, even if multiple, anonymous GPS Positions are lining up for a potential route. Furthermore these approaches do not take into consideration, that leaving a mix zones on a specific place (e.h. office or home) are strong indicators to a specific individual and leads to personalized information. Since we can not improve these method on the device itself and traceability is still possible, mix zones are not considered in the list of privacy patterns investigated here.

3 Related Work

Concerning location privacy, attacks and adversary models, an overview is given in [36]. In the context of privacy and provenance the risk of location information is investigated as one aspect [32]. Also in [7,35] location information is taken into account for assessing privacy risks.

User perceptions about privacy risks including risks concerning location privacy are the focus of a user study in [12]. The willingness of users to share location information depending on the context are investigated in [14,21,17,11]. Disclosure in dating apps is discussed in detail in [14]. [21] is describing the intrusiveness and consequences of location based ads. [17] introduces a mobile recommendation system for tourism considering privacy. [11] shows how users tend to think about their own location data to create a transparent bus delaying information service.

User ratings regarding location based service usefulness and mostly intrusiveness can be found in an early use case study [1]. Additional ethical questions about tracking mobile phone users were portrayed [34].

There are several technical approaches which address privacy enhancing technologies in the area of location information as e.g. mix zones [4] or the use of

pseudolocations to achieve k-anonymity [29]. Also there are approaches measuring the effectiveness of measurements to remove location information and the risk of reconstruction of this information [19].

Privacy enhancing patterns to improve location privacy are discussed in detail in [22]. Furthermore added fake requests to create dummy users for a different car route are explained [26]. Additionally the trade-off between location obfuscation and quality of service is described in [15].

4 Methodology

Based on the identified approaches in Section 3, a classification of utilized sensors resp. localization approaches, usage contexts and privacy perceptions concerning location privacy is developed. The most common approaches distinguish applications that persistently request and/or send location information of users, and those that allow users to send their location only upon request. On mobile phones several applications running in the background are steadily aware of users positions. We focus on application contexts and consider both types of applications in the classification. On request location aware services make use of certain privacy patterns as e.g. fixed time slots already obsolete.

For the consideration of typical contexts, several use cases are investigated in the following analysis. For each use case a standard solution is the basis of the investigation. There typical intervals of position requests and accuracy of the localization information are stated.

As a baseline of the analysis, the use cases are rated according to usefulness and intrusiveness. Usefulness and intrusiveness are criteria that are often investigated in the context of surveys about user acceptance of location tracking [1,11,12,21]. Usefulness or being 'useful' is described as 'can be used to advantage; serviceable; helpful; beneficial; often, having practical utility' by [10]. In the context of user studies usefulness was rated by the user and sometimes combined with the average number of uses per day of the given application. The notion 'intrusive' is defined as 'something that invades personal space, that becomes too involved or that comes too close without being invited' by [9]. Also concerning intrusiveness user perceptions are considered.

Whereas in most cases these user perceptions are mostly subjective, sometimes also general aspects as e.g. detecting the delay of buses [11] are taken into consideration. The rating of use cases is derived from these surveys. In addition the criterion criticality is considered. The original criticality is based on the analysis of use cases from a mainly technical perspective. There factors as times of localization and accuracy are taken into account to derive a criticality rating.

In a second step of the analysis, the impact of privacy-enhancing patterns on the evaluation of use cases is considered. To this aim, increase of privacy and also decrease of usability are investigated and the criticality in the context is derived.

5 Analysis

5.1 Use Cases of Location-Based Services

The following use cases give a broad overview of location-based services in daily life.

Social Events in City: Information about events in a certain area, e.g. a city or a region, is important for tourists and inhabitants. People organizing such events or organizations as city marketing or ticket sales organizations are interested in gaining attention to attract participants or increase ticket sales. Many implementations use exact locations and refresh rates are not transparent or even adjustable for users. A forced refresh of the information in the app by the user triggers an obvious update of the position, but in addition frequent updates in the background are triggered which is not transparent for the user.

ATM or store close by (on request): This describes a use case, where users can get position information of nearby stores or points of interest specified according to their current position. In this particular case users send their position and receive results on demand and are therefore not tracked most of the time.

ATM or store close by (on push): Instead of informing users only on request, in this use case they are informed periodically. Users could either be notified if they enter a certain area and the system knows and recognizes the device. Otherwise devices could send requests based on the current location all the time.

Close loop navigation (turn by turn): Besides classical offline navigation systems, where maps are updated via file transfer and accidents are transmitted via very high frequency (same as vhf radio stations), meanwhile systems with a permanent internet connection are often used, which collect position information of users for navigation and to detect traffic jams. Therefore positional information is updated permanently and as precise as possible.

Nearby friends: By this type of application information is provided, if a particular person of the friends list of the user is in a certain distance to the user. Positional updates are usually done every couple of seconds. Functions like these have become available in social networks, messengers and numerous dating apps, even more specific in the following use case. Sometimes there is information provided, how to decrease the localization accuracy from high to medium on mobile phones, but mainly due to less battery usage than to increase privacy.

Locate people on a map: In addition to the information that friends are nearby, maps are provided with position information of these friends. That does not only provide the distance of the persons to a user, but the specific location of them. Regarding privacy most of these applications provide possibilities to restrict the visibility of position and e.g. images. Irrespective of these visibility settings, providers store all of the positional information. Sharing location information happens in real time and is updated frequently with a high accuracy (see Fig. 2 [3]).

[3] Source: https://www.turn-on.de/tech/ratgeber/so-nutzt-du-die-neue-snap-map-in-snapchat-eine-anleitung-280917

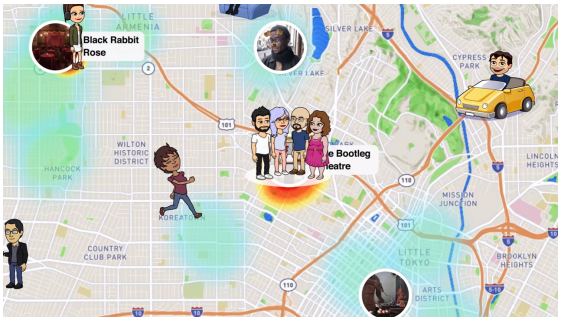

Fig. 2: Snapchats introduced Snap Map

Notification of traffic jam: In addition to turn by turn navigation the applications are notifying users about speed cameras ahead on the route, density of traffic, information about accidents and construction sites. This information is also taken into account in addition to the position of users to enhance route planning and the estimated time of arrival.

Location based ads: Location based advertisement is a very import part of targeted advertisement. Whereas targeted advertisement might happen while browsing through the web, it is also used in big shopping centers to track customer locations [23]. Beside tracking when customers enter or leave the shopping center, also their routes through the building might be tracked. User profiles could be derived by common fingerprinting approaches.

Location based games: Location based games are a recent trend. The general aim is to reach a specific position, earn points and collect achievements. Well-known examples are games as "Pokémon GO" (see Fig. 3(b)[4]) or "Harry Potter Wizards Unite" (see Fig. 3(a)[5]). Games are based on collectibles that are randomly placed on the map. These items are necessary for a good gaming experience and a virtual progress. They can be found while walking around the environment as the users characters in the game and adapt their positioning based on your real position and movement. Therefore positional information about the user is collected quite frequently and with high accuracy. The usefulness of that type of applications is quite subjective since it is a game and merely fun is the main purpose.

Location during emergency call: Transmitting the location during an emergency is a special use case taking location information into consideration. Emergency call (eCalls) is a technology transmitting important vehicular data e.g. airbag deployment, impact sensors, but also location data to the authorities in case of an emergency. This technique is mandatory for cars that are sold in the European Union since April 2018. Transmission of data happens only once in case of an accident and is highly accurate.

[4] Source: https://nianticlabs.com/de/support/pokemongo/

[5] Source: https://www.imore.com/harry-potter-wizards-unite-what-are-inns-and-how-do-they-work

(a) Harry Potter Wizards Unite

(b) Pokémon GO

Fig. 3: Location Based Games

5.2 Analysis of Typical Realizations of Use Cases

The evaluated use cases represent a broad variety and controversial necessity of stated applications. While differentiation between the type of localization were not made especially in these use cases, the types of localization and the place (e.g. indoor or outdoor) would lead to no difference since accuracy and the times of localization would be similarly realized in both settings.

The localization method and therefore the place of calculation implies additional threats besides location leakage. Based on [12] location leakage (and therefore probably other data e.g. from an IMU) is less crucial than image leakage which could happen if visual localization is obtained by vulnerable cloud services. In Table 2 these ratings are summarized.

As a first step of the analysis, the use cases presented in section 5.1 are evaluated based on surveys about user acceptance of location tracking [1,11,12,21] and typical technical realizations.

5.3 Privacy Patterns in Location Based Services

In the second step of the analysis the impact of applying privacy patterns for localization information is investigated. Therefore changes for intervals of localization and accuracy are considered and the implication on privacy is evaluated. In addition it is also important to consider changes to the usability resp. usefulness of the services, since these approaches minimize or obfuscate data to increase privacy.

criteria	Use Cases				
	social events in city	ATM close by (request)	ATM close by (push)	close loop navigation	nearby Friends
Usefulness	+1	+3	+2	+3	+2
Accuracy Times of Loc.	10m 30s	10m once	10m 10s	10m 1s	10m 5s
Intrusiveness	-3	-2	-3	-2	-3
Criticality	-4	-2	-4	-3	-4

criteria	Use Cases				
	Locate people on map	notification traffic jam	location based ads	location based games	location during emergency
Usefulness	+2	+3	+1	+2	+4
Accuracy Times of Loc.	10m 5s	10m 1s	10m 5s	10m 1s	10m once
Intrusiveness	-4	-2	-4	-3	-1
Criticality	-4	-3	-4	-4	-1

Table 2: Use Cases and their Usefulness (from +1 to +4), Intrusiveness (from -1 to -4) and Criticality (from -1 to -4).

For each use case and privacy pattern, the resulting criticality of the use case is rated as follows based on the other criteria for the use case:

$$Criticality = UF + I + Crit_{orig} + IoP + DoU \tag{1}$$

The criticality is described as the sum of the previous weighted elements as seen in (1). There UF denotes UseFulness, I is Intrusiveness, IoP describes the Increase of Privacy, DoU the Decrease of Usability. All elements were weighted corresponding to the weights stated in table 3. The evaluation of all parameters and the overall criticality is described below and summarized in table 4.

Element	Weight	normalized
Usefulness	0	0
Intrusiveness	1	0.14
Original Criticality	3	0.43
Increase of Privacy	1	0.14
Decrease of Usability	2	0.29

Table 3: Applied weights to the elements in equation 1

The weights are chosen based on the corresponding considerations. To minimize personal preferences of users the initial usefulness is not considered by choosing the weight for usefulness as 0, since the application is already used and hence considered as useful. Since the overall intrusiveness of the application itself still has an impact even if privacy patterns are applied, the initial intrusiveness has the weight of 1. It was tried to enhance given intrusiveness, by a technical view e.g. location aware or location tracking, on demand or continuing location data resulting in the original criticality of the use case. This original criticality

is one of the most important factors resulting in a weighting of 3. We chose the Increase of Privacy weight as 1 since it is important that privacy patterns lead to an increase of privacy. Additionally we decided to choose a higher weight of 2 for Decrease of Usability taking the users point of view into consideration. Since privacy patterns will not be applied, resp. users will not consider using an application that is barely usable anymore.

Location based services for identifying **social events in a city** is a good example for improvements concerning privacy. Standard localization (e.g. via GPS) is pretty accurate (around 10m) and might be done every 30s (depending on settings in the app or chosen by the developer). Decreasing the accuracy to around 20km could be coped by providing more information resulting in more events. This results in more flexibility for users but also in the need of filtering the results more thoroughly manually and thus decreasing the usability. Overall this is quite a viable strategy to increase privacy.

Adding a slight variable delay to location data in a non time-critical application has no substantial impact and hence leads to mainly no decrease in usability but also only to a slight increase in privacy. A larger delay would improve privacy farther but also lead to a further decrease of usability. For applications based on information that is merely static, fixed time slots, e.g. every 3 hours or even only once a day, seems to be a viable option. Especially events which need a thorough preparation and sometimes additional approvals are typically known far longer than a day before. Therefore larger time slots would be manageable. Short term updates of certain events could be achieved by subscribing to events which users intend to visit. Even if this might lead to different private issues, really tight localization timers or position request become obsolete. Furthermore planning for a trip might be coped with a search function for cities or areas. Moreover adding noise to the location data, like requesting data for multiple cities across the country, might be a good approach to increase privacy as well, since the service is not directly disrupted by requests based on different locations. The drawbacks are that more data has to be filtered on the device and also the increased work load for sending these data and handling of requests on the server side. Also dummy users could be inserted. From the service providers point of view the load only increases if the number of users is substantially increased by dummy users.

Regarding **ATMs or stores close by (on request)** one can see that the original criticality in contrast to the **(on push)** application is lower. This is due to the fact that updates and positional information are only sent upon manual request of users, which leads to a high grade of control. On the other hand frequently requesting data based on users movements might be more useful for some but results in a higher criticality.

In both cases delaying and decreasing the times of localization helps in general but results only in a small increase of privacy. Using big time gaps increases privacy further, but results also in a substantial decrease of usability. While aligning the positional information to an underlying grid might be a good idea,

Use Case							
criteria	normal	Points on Grid	delay slight (x s)	delay big (x h)	time slots - every (x min)	time slots - every (x h)	Dummy Users
social event in city							
times of localization	30s	30s	+10s	+1h	180min	24h	30s
accuracy	10m	20km	10m	10m	10m	10m	10m
increase of privacy	none	+3	+1	+2	+2	+3	+4
decrease of usability	none	-1	-1	-2	-2	-2	-1
criticality	-4	-2	-2	-3	-3	-2	-2
ATM or store close by (on request)							
times of localization	once	once	+10s	+1h	once	once	once
accuracy	5m	5km	5m	5m	5m	5m	5m
increase of privacy	none	+2	+1	+3	x	x	+4
decrease of usability	none	-3	-2	-4	x	x	-2
criticality	-2	-2	-2	-2	x	x	-1
ATM or store close by (on push)							
times of localization	10s	10s	+10s	+1h	5-10min	1h	10s
accuracy	5m	5km	5m	5m	5m	5m	5m
increase of privacy	none	+2	+1	+3	+2	+3	+4
decrease of usability	none	-3	-1	-3	-2	-3	-2
criticality	-4	-3	-2	-3	-2	-3	-2
close loop navigation (turn by turn)							
times of localization	1s	1s	+10s	+1h	1min	1h	5s
accuracy	5m	250m	5m	5m	5m	5m	5m
increase of privacy	none	+2	+1	+2	+2	+3	+3
decrease of usability	none	-3	-3	-4	-3	-4	-1
criticality	-3	-2	-2	-3	-2	-2	-1
nearby friends							
times of localization	5s	5s	+10s	+1h	5-10min	1h	5s
accuracy	100m	10km	100m	100m	100m	100m	100m
increase of privacy	none	+3	+1	+2	+2	+3	+3
decrease of usability	none	-2	-1	-4	-2	-4	-3
criticality	-4	-2	-2	-3	-2	-3	-3
locate people on a map							
times of localization	5s	5s	+10s	+1h	5-10min	1h	5s
accuracy	100m	10km	100m	100m	100m	100m	100m
increase of privacy	none	+3	+1	+2	+2	+3	+4
decrease of usability	none	-3	-1	-3	-2	-3	-4
criticality	-4	-2	-2	-3	-3	-3	-3
notification of traffic jam							
times of localization	5s	5s	+10s	+1h	5min	1h	5s
accuracy	100m	10km	100m	100m	100m	100m	100m
increase of privacy	none	+3	+1	+3	+3	+4	+4
decrease of usability	none	-2	-1	-3	-2	-3	-4
criticality	-3	-2	-2	-2	-2	-2	-2
location based ads							
times of localization	5s	5s	+10s	+1h	5-10min	1h	5s
accuracy	5m	5km	5m	5m	5m	5m	5m
increase of privacy	none	+2	+1	+3	+3	+3	+4
decrease of usability	none	-3	-1	-3	-2	-3	-1
criticality	-4	-3	-3	-3	-2	-3	-1
location based games							
times of localization	1s	1s	+10s	+1h	5min	1h	1s
accuracy	10m	1km	10m	10m	10m	10m	10m
increase of privacy	none	+2	+2	+2	+3	+4	+4
decrease of usability	none	-3	-2	-3	-2	-3	-4
criticality	-4	-3	-2	-3	-2	-2	-3
location during emergency call							
times of localization	once	once	+10s	+1h	once	once	once
accuracy	1m	50m	1m	1m	1m	1m	1m
increase of privacy	none	+2	+1	+1	x	x	+4
decrease of usability	none	-4	-3	-4	x	x	-4
criticality	-1	-2	-3	-3	x	x	-2

Table 4: Analysis of Criticality, Privacy and Usability - increase of privacy from +1 (worst) to +4 (best), decrease of usability -1 (minimal) to -4 (disrupted) and criticality from -1 (minimal) to -4 (bad) - or not applicable (x).

localization frequency would be still high. Further adding dummy users has the same effect as in the previously described use case.

A reasonable approach could be to combine lower times of localization with a lower accurate positioning and in addition adding dummy users if possible. Also since positions do not change regularly, information might be saved locally on the device beforehand. An update of these stored positions could still be triggered manually beforehand and distance calculations etc., could be done locally.

Turn by Turn navigation relies on close loop positional data to guide users around the streets. While probably not all positional information is directly sent to the service provider during navigation, some information would often be collected and sent to the service provider at least afterwards to improve quality of service. Aligning the estimated positions on a grid could make navigation much more difficult. The current position might jump between streets, or blocks, if the granularity of the grid is not adequately chosen. Therefore this is problematic regarding usability since the service might e.g. confuse intersections. Also the current direction and velocity would be impossible to calculate due to inaccurate positions if no additional sensor data is available.

Adding delays complicates navigation for the user as well since the whole process starts lagging. Fixed time slots for orientation might work, but the user would have to remember turns in between updates which makes it more complicated to navigate in cities. Adding Dummy Users depends on how the additional users are aligned. If there is just a random cloud of additional data around a certain position all the time, the original route is still traceable. Furthermore realistic routes have to be simulated.

Nearby Friends, **locate people on a map** and the **notification of traffic jams** have similar problems. Decreasing the accuracy of positional information substantially will render the service nearly unusable. Most of these applications update their positional information too often (e.g. people on a map are usually updated every 2 seconds). These update cycles could be lowered and still offer full functionality. Adding dummy users could be a possibility, but incorporates the risk of distorting these services.

Location based games might lead to another problem. While delaying is annoying in some games, adding dummy users could lead to a disruptive or even not playable game anymore since some of the games measure the distance and time between positions. Some games restrict, penalize or punish for fast movement. Sending multiple positions might be colluding with the game itself, since most actions of the user have to be confirmed by the server, before a certain progress in the game is possible. Furthermore it could be considered as a way of cheating. Adding a big delay might decrease the usability substantially. Hence decreasing the accuracy might be a more viable option.

The last use case investigated is the **emergency call**. Decreasing accuracy as well as only sending positions in fixed, predetermined time slots, delaying the data transmission or adding additional dummy positions might lead to delays or confusion for emergency forces. Applying privacy patterns in that use case might be questionable for such a crucial task due to a low original criticality rating.

6 Discussion and Conclusion

Location-based services are already used ubiquitously and constitute an important innovation in the area of smart services. Especially the success of smartphones and the development of AR devices as the Microsoft Hololens foster this trend. Therefore it is important to develop frameworks for location privacy and to reduce the privacy risk based on context and user perceptions.

Location requests triggered by users ensure the lowest intrusiveness, since the user knows about sending current location information and can control these types of requests. Certainly retrieving data on request is preferable, persistent requests could be pruned. For example fixed time slots for providing the same kind of information can be useful. Neglecting computational power adding noise and therefore additional requests to services is a quite reliable way as long as the service is still usable. Otherwise decreasing accuracy should be kept in mind as well since applications often update positions every couple of seconds close enough to tenth of meters, even if it is not necessary.

In general it is preferable to compute positions and routes on the local device instead of employing cloud services to minimize data. But as summarized in Table 1, a variety of localization methods are not suitable to be calculated on a smart phone only. But even if cloud computation is needed, data minimization should be a top priority. Positional data minimization might be accomplished as well, if only edges of a building are send at a certain location, triggered by the user.

The development and investigation of privacy patterns for location privacy is an important topic for future research. A central problem is that often the usefulness decreases substantially such that some services are nearly rendered unusable. Based on this general analysis, it would be important to investigate privacy perceptions of users in different usage contexts in more detail..

Acknowledgment This work was supported by the Federal Ministry of Education and Research (BMBF) as part of SmarteInklusion (01PE18011C).

References

1. Barkhuus, L., Dey, A.K.: Location-based services for mobile telephony: a study of users' privacy concerns. In: Interact. vol. 3, pp. 702–712. Citeseer (2003)
2. Bellavista, P., Küpper, A., Helal, S.: Location-based services: Back to the future. IEEE Pervasive Computing 7(2), 85–89 (2008)
3. Beresford, A.R., Stajano, F.: Location Privacy in Pervasive Computing. IEEE Pervasive computing 2(1), 46–55 (2003)
4. Beresford, A.R., Stajano, F.: Mix zones: User privacy in location-aware services. In: IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second. pp. 127–131. IEEE (2004)
5. Boutet, A., Mokhtar, S.B., Primault, V.: Uniqueness assessment of human mobility on multi-sensor datasets (2016)

6. Cipolla, R., Robertson, D., Tordoff, B.: Imagebased localization. In: Proc. Int. Conf. Virtual Systems and Multimedia. vol. 2004 (2004)
7. De, S.J., Le Métayer, D.: Priam: a privacy risk analysis methodology. In: Data Privacy Management and Security Assurance, pp. 221–229. Springer (2016)
8. De Montjoye, Y.A., Hidalgo, C.A., Verleysen, M., Blondel, V.D.: Unique in the crowd: The privacy bounds of human mobility. Scientific reports 3, 1376 (2013)
9. Dictionary, Y.: Definition of "intrusive".". Retrieved from https://www.yourdictionary.com/intrusive (2015)
10. Dictionary, Y.: Definition of "useful.". Retrieved from https://www.yourdictionary.com/useful (2015)
11. Dou, E., Eklund, P.W., Gretzel, U.: Location privacy acceptance: attitudes to transport-based location-aware mobile applications on university campus (2016)
12. Felt, A.P., Egelman, S., Wagner, D.: 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. pp. 33–44. ACM (2012)
13. Finn, R.L., Wright, D., Friedewald, M.: Seven types of privacy. In: European Data Protection: Coming of Age, pp. 3–32. Springer (2013)
14. Fitzpatrick, C., Birnholtz, J., Brubaker, J.R.: Social and personal disclosure in a location-based real time dating app. In: 2015 48th Hawaii International Conference on System Sciences. pp. 1983–1992. IEEE (2015-01), http://ieeexplore.ieee.org/document/7070049/
15. Gardner, Z., Leibovici, D., Basiri, A., Foody, G.: Trading-off location accuracy and service quality: privacy concerns and user profiles. In: Localization and GNSS (ICL-GNSS), 2017 International Conference On. pp. 1–5. IEEE (2017)
16. Garon, M., Boulet, P.O., Doironz, J.P., Beaulieu, L., Lalonde, J.F.: Real-time high resolution 3d data on the hololens. In: 2016 IEEE International Symposium on Mixed and Augmented Reality (ISMAR-Adjunct). pp. 189–191. IEEE (2016)
17. Gavalas, D., Konstantopoulos, C., Mastakas, K., Pantziou, G.: Mobile recommender systems in tourism. Journal of network and computer applications 39, 319–333 (2014)
18. Hito, G.: Overlaying virtual scale models on real environments without the use of peripherals (2018)
19. Hossain, A., Quattrone, A., Tanin, E., Kulik, L.: On the effectiveness of removing location information from trajectory data for preserving location privacy. In: Proceedings of the 9th ACM SIGSPATIAL International Workshop on Computational Transportation Science. pp. 49–54. ACM (2016)
20. Hübner, P., Weinmann, M., Wursthorn, S.: Marker-based localization of the microsoft hololens in building models. International Archives of the Photogrammetry, Remote Sensing & Spatial Information Sciences 42(1) (2018)
21. Ketelaar, P.E., Bernritter, S.F., van Woudenberg, T.J., Rozendaal, E., Konig, R.P., Hühn, A.E., Van Gisbergen, M.S., Janssen, L.: "opening" location-based mobile ads: How openness and location congruency of location-based ads weaken negative effects of intrusiveness on brand choice. Journal of Business Research 91, 277–285 (2018)
22. Krumm, J.: A survey of computational location privacy. Personal and Ubiquitous Computing 13(6), 391–399 (2009)
23. Li, K., Du, T.C.: Building a targeted mobile advertising system for location-based services. Decision Support Systems 54(1), 1–8 (2012)

24. Ma, C.Y., Yau, D.K., Yip, N.K., Rao, N.S.: Privacy vulnerability of published anonymous mobility traces. IEEE/ACM transactions on networking (TON) 21(3), 720–733 (2013)
25. Meng, P., Fehre, K., Rappelsberger, A., Adlassnig, K.P.: Framework for near-field-communication-based geo-localization and personalization for android-based smartphones-application in hospital environments. In: eHealth. pp. 9–16 (2014)
26. Meyerowitz, J., Roy Choudhury, R.: Hiding stars with fireworks: location privacy through camouflage. In: Proceedings of the 15th annual international conference on Mobile computing and networking. pp. 345–356. ACM (2009)
27. Nister, D., Naroditsky, O., Bergen, J.: Visual odometry. In: Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2004. CVPR 2004. vol. 1, pp. 652–659. IEEE (2004), http://ieeexplore.ieee.org/document/1315094/
28. Parra, I., Sotelo, M.A., Llorca, D.F., Ocaña, M.: Robust visual odometry for vehicle localization in urban environments. Robotica 28(3), 441–452 (2010)
29. Peng, T., Liu, Q., Wang, G.: Enhanced location privacy preserving scheme in location-based services. IEEE Systems Journal 11(1), 219–230 (2014)
30. Qu, X.: Landmark based localization: Detection and update of landmarks with uncertainty analysis p. 191 (2016-10)
31. Rauschnabel, P.A., Rossmann, A., tom Dieck, M.C.: An adoption framework for mobile augmented reality games: The case of pokémon go. Computers in Human Behavior 76, 276–286 (2017)
32. Reuben, J., Martucci, L.A., Fischer-Hübner, S., Packer, H.S., Hedbom, H., Moreau, L.: Privacy impact assessment template for provenance. In: 2016 11th International Conference on Availability, Reliability and Security (ARES). pp. 653–660 (2016-08)
33. Swank, A.J.: Localization using visual odometry and a single downward-pointing camera (2012)
34. Taylor, L.: No place to hide? the ethics and analytics of tracking mobility using mobile phone data. Environment and Planning D: Society and Space 34(2), 319–336 (2016)
35. Van Zoonen, L.: Privacy concerns in smart cities. Government Information Quarterly 33(3), 472–480 (2016)
36. Xue, M., Liu, Y., Ross, K.W., Qian, H.: I know where you are: thwarting privacy protection in location-based social discovery services. In: 2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). pp. 179–184. IEEE (2015)
37. Zhou, B., Li, Q., Mao, Q., Tu, W., Zhang, X.: Activity sequence-based indoor pedestrian localization using smartphones. IEEE Transactions on Human-Machine Systems 45(5), 562–574 (2014)