Supporting digital sovereignty in LBS with a digital learning tool
PhD Proposal

Sven Heitmann

1 Introduction

Nowadays, a lot of people are using Location based services (LBS), mobile smartphone applications that use personal location information (PLI) in order to tailor a digital service to the users' current context. Some examples are navigation systems, social media apps, dating apps or local recommender systems. Users tend to share their PLI freely with such LBS although this location information is extremely sensitive. Already with comparatively simple mechanisms, home and work location can be inferred [20]. In addition, more sensitive locations like regular visits to hospitals or night clubs [35], which give insights into health status or sexual orientation, might be inferred. Hence, when a user shares their PLI with a service provider, their privacy regarding location might be harmed. Bargiotti et al. define location privacy as "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" [6]. In the recent years, a number of technological protection mechanisms have emerged that try to protect the users' PLI against inferences or attacks, as highlighted in a variety of publications [21, 26, 14, 35, 11].

Nevertheless, even with protection mechanisms as proposed in the literature, users serve currently only as data providers and are not seen as active participants that can make informed decisions about sharing PLI with a LBS. We argue that this situation results is a severe lack of *digital sovereignty*. While the concept of sovereignty is traditionally understood as a state executing supreme, independent authority, Misterek defines an extended concept of digital sovereignty on a society level. He implies that digital sovereignty is only existing, when the society takes part in the organization of digitalization [29]. Among different kinds of sovereignty categories and definitions, Cauture and Toupin identify "personal technological sovereignty" as "control of an individual over her data" [17]. In order to take control over their data, users first need to be informed and aware about location privacy and the implications of sharing PLI. In reality, most people are not really aware of the implications. Research on user perception of location privacy has also shown that some users do not give their location privacy a high (monetary) value and willingly share their PLI [18, 31]. Even if they care about their location privacy, users are often not taking any actions to protect it [16]. Nevertheless, some people would like to have more control over their location data [25] but would need the appropriate tools to exert this control like, for example, privacy management tools [1] with appropriate user interfaces [4]. Those tools should be easy to understand [13] and should be tailored to their needs [28]. Still, a lot of users lack basic information and location privacy knowledge, privacy skills and awareness of the risks [30].

Although some researchers demand basic educational tools [16], little focus has been put on how we can actually educate people about location privacy, raise awareness and design and evaluate tools that facilitate learning in that area. At this point, we are only aware of three systems that explicitly aim at educating users about location privacy: A labware for undergraduate students [27] for classroom use, the "FindYou" system from Riederer et al. [32] that gives users the opportunity to explore their location tracks and demographics derived from them in an online auditing tool and a similar, more recent system developed by Boutet et al. [12] that enables users to apply some data sanitation processes and explore, how the risk of inferences based on their PLI changes. Although promising, user studies with those system were very limited and it is thus open if such educational systems actually serve their purpose.

Hence, we argue that the current state of digital sovereignty about PLI is inadequate. In order to change this and to facilitate a better incorporation of users and strengthen their role, designers of future LBS need a better understanding about their users' knowledge, understanding, perception of threats and their ability to learn about the concepts of location privacy and digital sovereignty. This leads to the following question that will be addressed in the proposed dissertation: *How can digital sovereignty be supported with a digital learning tool?*

Sven Heitmann
Institute for Geoinformatics, Heisenbergstraße 2, 48149 Münster, e-mail: sven.heitmann@uni-muenster.de

2 Related Work

2.1 Basic concepts

Over the last two decades, researchers identified three four main elements in location privacy research, namely regulations [21, 11], ways to attack location privacy [21, 26, 14, 35, 11], mostly technical defense mechanisms [21, 26, 14, 35, 11], and the role and perception of end users [26, 14, 11]. One very prominent and recent example for regulations is the European General Data Protection Regulation (GDPR)[1] that requires entities who collect and process user data to do this in certain ways like, for example, obtaining the users' informed consent to collect their location data [34]. Although in practice, such regulations are often hard to understand and implement in practice by developers [5]. Previous research has shown that location data is very sensitive. By analyzing a users location data (e.g. collected by a service provider), additional information like home and work address [20], frequently visited points of interest [12] or a general demographic profile [32] can be inferred. In order to mitigate such threats of inferring additional information, a number of technical defense mechanisms has emerged that aim to protect the location privacy of LBS users when issuing requests to a service provider. Some popular examples are position dummies [24], mix zones [10], k-anonymity [22] or spatial obfuscation [3]. A very recent trend is the concept of differential privacy [36]. For position dummies, the user's device does not send a single location request to a service but multiple dummy locations in addition to hide her true location [24]. In the mix zones approach presented by Beresford and Stajano pseudonyms are used to send requests to a service provider. When entering a mix zone, they stop sending requests and exchange their pseudonym with another user to protect their privacy [10]. In a system that implements spatial k-anonymity, a user does not send their real location but an area that contains at least k-1 users together with a pseudonym so that the service provider can not distinct who of those users has send the request [22]. In spatial obfuscation, not the real user location is sent to a LBS but some kind of degraded location information, e.g. a circular area that contains the real user location [3].

2.2 User related research

User related research regarding location privacy is often centered around common themes, namely user concerns [8, 7, 37, 25], location sharing preferences [2], preferences for privacy mechanisms in the context of location sharing [13, 33, 9, 4], user preferences for trade offs they are willing to make regarding privacy and benefits through service provision [16], value attached to location privacy or location data [18, 31], general awareness of the topic [34, 12], perception of location privacy [23] or mental models of data usage in the context of mobile apps [28]. Some authors explicitly look at privacy knowledge and skills [30] or change of behaviour and awareness [1].

To investigate those topics, researchers applied a number of methodologies. Quite often, studies with stand-alone questionnaires [18, 23, 37, 25, 16], sometimes carried out via online crowdsourcing systems [28, 31] or interviews [34] were conducted. Common setups consist of pre-study-interviews [7, 4] or -questionnaires [9, 30, 1], followed by some kind of study. For such studies, imaginative LBS with journal studies [8], experience sampling [2] or more practical, mobile study setups with deployed mobile applications that track the users' location, like a campus navigation system [7], geotagging service [13] or the Locaccino location sharing system [33, 9] have been applied. Some developed applications are installed on the users' phones and offer additional information about other apps using the users' PLI [1]. Other studies use local systems that analyse the the users' own data [12] or artificially created scenarios in semi-realistic lab environments [4]. Another common approach are observation studies where users interact with a system [7, 30, 34] while being observed by a researcher. In a more artificial setting, online crowdsourcing studies with artificial scenarios presented via application screenshots [28, 31] were conducted. Studies that subject users to some kind of location privacy experience, are quite often followed by a post-study questionnaire [8, 33, 9, 1] or interview [7, 30, 1, 4].

Results reveal that some users are initially concerned about their location privacy, but when they actually use an LBS, their level of concern drops. [7]. In addition, privacy concerns are not a cause for not using a LBS. Even if users have privacy concerns, they might still use LBS, for example, due to social pressure [37]. On the other hand, if users are in general more inclined to having control, their concern about location privacy is also higher [25]. Regarding location sharing preferences with other users some people never, some always and some share their location depending on the context, which indicates the need for flexible user interfaces [2]. If privacy protection mechanisms are exposed to end users, they should be easy to understand [13], should cater for the users privacy preferences depending on their context [33] like, for example, time of the day or user location [9]. The work of Ataei et al. revealed that, if designed properly, users are in general inclined to make use of location privacy management mechanisms [4]. Even if users are aware of risks related to sharing their location data, they often do not take necessary steps

[1] Regulation 2016/679 of the European Parliament and the Council, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN, accessed 16 July 2021

to address these [16]. In addition, users put very little monetary value to their location privacy [18, 31]. Others found out that the users' expectations and purpose of sensitive information usage have great impact on users' feelings, trust and decisions. So properly informing users could actually ease their privacy concerns [28]. The study of Park et al. has revealed that many users lack basic information and location privacy knowledge, privacy skills and awareness of the related risks. Although users are highly familiar with their mobile devices, this does not translate into actionable knowledge [30]. Even if users are given a system like a permission manager as in [1] and use the controls that are offered, their overall awareness of collected data remains limited. On the other hand nudges motivate users to take action [1].

We have seen that the general awareness for LP and related skills not very pronounced, users tend to give little value to their LP and understand potentially very little about the related risks. At the same time, control over location data and sharing mechanisms does seem to play a role. Here, we see a need for educational tools. From a methodological point of view, many studies rely on interviews questionnaires or artificial scenarios. We argue for the need for more practical studies, where an actual system is used in more realistic environment.

2.3 Educating users about location privacy

Little work has been done in the area of developing and evaluating systems that explicitly educate people about location privacy. This is especially important, since there seems to be a lack of awareness and privacy related skills. Riederer et al. developed "FindYou", a demo of a web based auditing system where users can upload their own location data from Foursquare, Instagram or Twitter. It offers the user the possibility to explore their location data and visualizes how service providers can threat their users' location privacy by analysing frequently visited locations. It does not only show them their home location but does also predict demographic information like race, income or age based on publicly available US census data. In addition, it allows users to edit their information and remove data points to illustrate how the the predicted demographic information changes [32].

Another online tool to raise the users awareness about the threat of profiling based on their location traces has been demonstrated by Boutet et al. Similar to [32], users can upload their Google location history. The system then confronts the user with inferences made based on the data like, for example, regularly frequented points of interest (e.g. home and work place) or predictions of gender and salary (based on census information). It does also offer the ability to apply a location privacy-preserving mechanism and explore its effects on the inferences. Although the authors mention a user survey, they do not report any results [12].

Li et al. have developed a labware for educating university students and tested it in a small user study. Their system consist of three components. A simple location based service allows users to request landmarks based on their current location from a LBS server. The LBS, implemented as an Android app, allows users to apply different levels of anonymizing their location upon a request. The system provides a simple overview of the trajectories of the user trajectories and and gives the students the opportunity to experience the the trade-off between privacy and service quality. A pilot indicates an increase in awareness and interest in the topic of location privacy after using the labware [27].

Little work has been done in using technical means to educate users and research how they can understand and apply protection mechanisms. Hence, there is clear gap regarding digital, educational tools to find out if and how users can be educated about LP. This gap leads to research activities defined in the next section.

3 Research questions and objectives

The proposed dissertation investigates how digital sovereignty regarding PLI in LBS can be supported with digital, educational means and addresses the following research question:

- RQ 1 What is the status quo of location privacy in research and practice?
- RQ 2 What is the users' current perception of location privacy?
- RQ 3 Which interactive means are suitable for conveying information about the aspects of location privacy and digital sovereignty?

RQ 1 will be addressed by conducting a literature research to identify key concepts of location privacy and digital sovereignty and by analysing existing apps for interaction patterns for giving informed consent to location access. To answer RQ 2 and RQ 3, a digital learning tool will be developed that subjects and informs users about the risks and consequences of location sharing and concepts of location privacy and digital sovereignty (e.g. taking control over their data). This mobile smartphone application will then be used to conduct user studies to investigate the current user perception of location privacy and to develop and evaluate means of educating users about location privacy and digital sovereignty.

4 Research activities and expected results

The proposed research activities are part of the SIMPORT[2] project and therefore group activities where multiple researchers are involved. Where already applicable, for potential publications it is highlighted if the author of this proposal is the first author.

4.1 Study 1: Background information

To form a broader understanding of the current status quo, the first studies set the theoretical and practical background for the following studies and addresses RQ 1: What is the status quo of location privacy and digital sovereignty in research and practice?

4.1.1 Study 1.1: Elicit status quo of location privacy in literature

Since we want to educate users about LP and digital sovereignty, it is important to identify core concepts first. Those will then inform the following activities. Here, the following research questions will be addressed:

- RQ 1.1 What is the status quo of location privacy in research?
  - RQ 1.1.1 What is the current state of the art in location privacy?
  - RQ 1.1.2 What are the key concepts in location privacy and how are they linked with each other?
  - RQ 1.1.3 To what degree is digital sovereignty considered in location privacy research?

Those questions are approached via a structured literature research and a review of survey papers. Due to the large body of work already existing in the field, an emphasis is put on synthesizing common concepts and trends from survey papers on location privacy. In addition, typical attack and defense mechanisms will be extracted. The expected results are an overview of the status quo in research. The extracted key concepts will be developed into a conceptual model to highlight relationships between users, service providers, attackers, protection mechanisms and means of information and control. Another result will be a structured collection of attack and defense mechanisms. Survey papers cover past work, so the results of the review might be slightly limited and not cover the latest technical developments in location privacy. The literature research has been conducted and the results of the review of survey papers is currently synthesized into a research paper that will be handed in at Journal of Location Based Services in September 2021. The author of this proposal will be a co-author.

4.1.2 Study 1.2: Analysis of commercial location based services

Since the aim of this work is to provide means for educating and informing users with digital means that could be integrated into future LBS, it is analyzed how information about location privacy and control over location access is currently presented by mobile applications. The following research questions will be addressed:

- RQ 1.2 How do current industry practices align with the concept of digital sovereignty?
  - RQ 1.2.1 What is the current state of informed consent for sharing location data with a LBS?
  - RQ 1.2.2 To what extent do current practices support digital sovereignty?

One core element of the GDPR is that users need to give *informed* consent to data collection and processing [34], which we argue is a vital part of digital sovereignty. Hence, we look at how mobile LBS request informed consent for accessing the users' PLI. 42 popular mobile LBS from the app stores on Android and iOS are analyzed by two independent raters with the aim to identify common approaches and reveal dark patterns in the user interface design. Dark patterns are user interface designs that trick users into performing an action they were initially not inclined to perform [19]. To evaluate the consesus between the two raters, an inter-rater reliability measure like Cohen's weighted kappa [15] will be reported. The contribution of this study is an overview of the common patterns for requesting informed consent and an identification of gaps on the way towards more digital sovereignty for users. However, this analysis provides only a snapshot in time in the fast changing landscape of mobile applications and operating system user interfaces. This research activity is currently in the last stages and the results will be submitted to the Conference on Location Based Services in August 2021. For this paper, the author of this proposal has the main-authorship.

[2] Sovereign and Intuitive Management of Personal Location Information, https://simport.net/, accessed 12 July 2021

4.2 Study 2: Explorative deployment study with mobile learning tool

Previous research on user perception of LP was often executed in theoretical or artificial settings which might have influenced the responses. In addition, few systems were developed to explicitly educate people about LP. To educate people better about LP, research in a more realistic scenario is needed and the general approach of a mobile learning tool needs to be tested and evaluated. This explorative study aims to answer the following questions:

- RQ 2 What is the users current perception of location privacy?
  - RQ 2.1 What is the users knowledge about the risks and consequences of sharing their location data?
  - RQ 2.2 How do users perceive the associated risks?
  - RQ 2.3 How would users like to be educated about the aspects of location privacy and digital sovereignty?
- RQ 3 Which interactive means are suitable for conveying information about the aspects of location privacy and digital sovereignty?
  - RQ 3.1 How effective is a situated threat indicator for educating users about risks and consequences of sharing location data with a service provider?

To confront the users with the risks of sharing their location with a LBS, a digital learning tool for Android and iOS is developed that tracks the users' location, analyses their trajectory and subjects them to inferences based on the collected PLI. In the current iteration, it infers home and work location, similar to [20]. In the future, regularly frequented points of interest (POIs) will be presented. For privacy reasons, the location data is processed locally on the users device. This application will be used for a three-phase study: After deploying the app remotely to the users device, pre-study questionnaires or interviews will be performed to elicit the participants current knowledge and attitude towards LP. During a three week study time, a duration similar to the study of Benisch et al. [9], the app notifies the participants about inferences and displays them on a map as a "situated threat indicator". After this period, the participant will fill out another privacy questionnaire. This way, we want to investigate if their perception of LP has changed, gather feedback on the learning tool for future studies and study the users' preferences for being educated. Apart from the development and first evaluation of a novel way of educating users, the study will also serve as a test for the effectiveness of questionnaires (or interviews) to measure learning. As a limiting factor, the study setup might still be perceived as an artificial scenario. Combined with self-reporting before and after the study, the results might hence not reflect the users' true attitudes towards LP. Since the inferences are computed locally without additional sources, they do potentially not reflect the *real* potential of service providers attacking their users' LP by including other data sources. A possible outlet for handing in the results is the MobileHCI conference in early 2022. The author of this proposal will be main author.

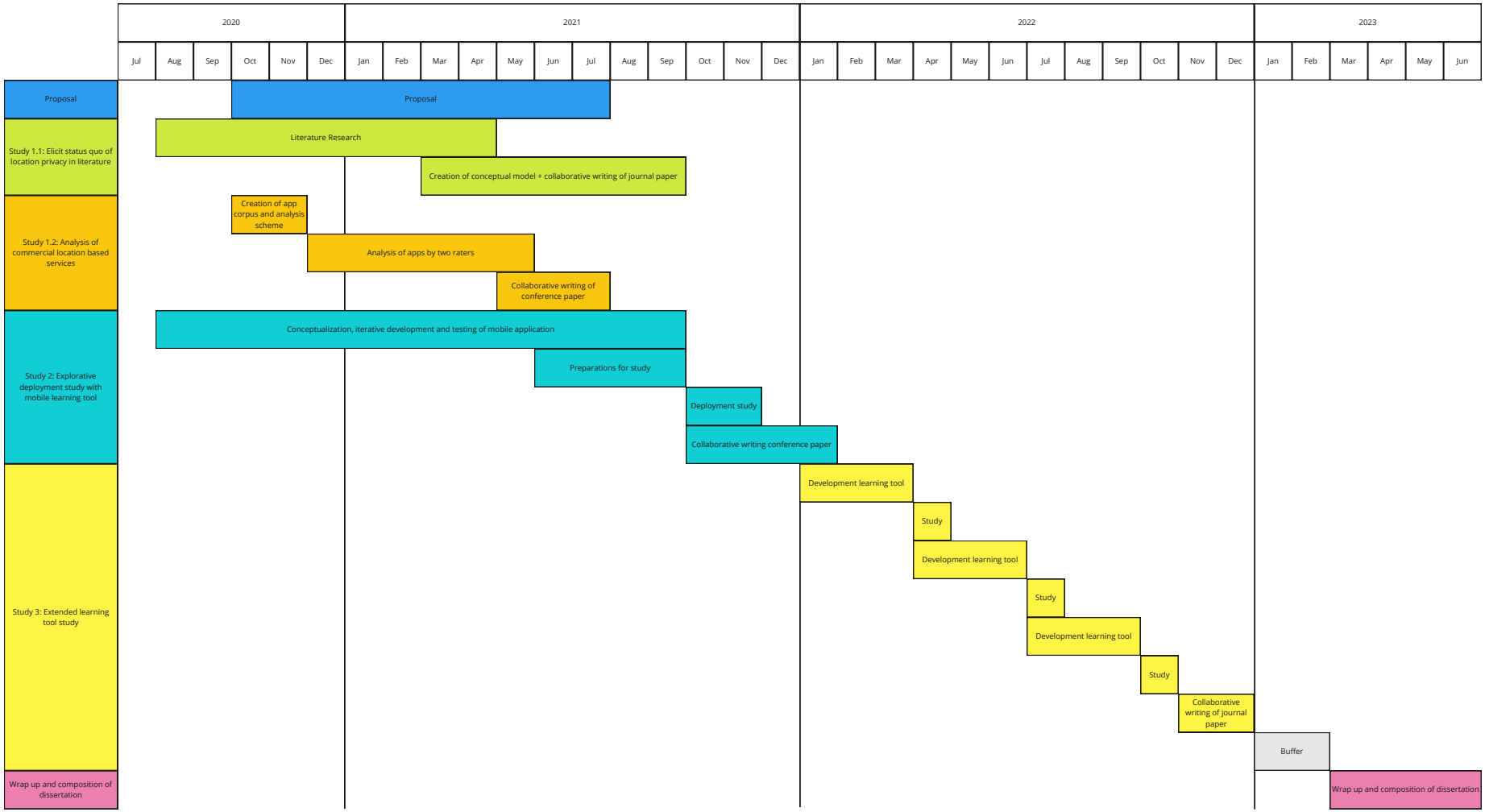
4.3 Study 3: Extended learning tool study

Taking the results of the first deployment study and assuming that the approach is confirmed, the learning tool will be further refined and used implement and evaluate more elaborate means to educate users. This leads to the following research questions:

- RQ 3 Which interactive means are suitable for conveying information about the aspects of location privacy and digital sovereignty?
  - RQ 3.3 How effective is the provision of information about general concepts of digital sovereignty in combination with a time slider for educating users about consequences of location sharing and possible protection mechanisms?

The design of the learning tool depends on the results of Study 2, hence only some possible ways of going forward are described here. The learning tool will be enhanced with simple mechanisms that support digital sovereignty by providing more control over their PLI and give the users the opportunity to learn about the underlying concepts that were identified in the Study 1.1. This activity will consist of multiple studies, for example, comparing similar systems in a mobile and local environment. Inspired by the work of Boutet et al. [12], simple control and protection mechanisms, like the possibility of adjusting the granularity of shared PLI, could be provided. In combination with a timeslider, the user could explore how exerting control over their data changes the risk of being subjected to inferences. The learning tool will be enhanced in multiple iterations. Each iteration will be evaluated with a small study where the results inform the next development steps. For each iteration, one could imagine two studies to compare a mobile study setup with the users' own data similar to Study 2 and a local, short term study in a semi-realistic lab environment with artificial data, similar to the work of Ataei et al. [4]. The proposed studies should provide insights into users' preferences for control mechanisms over PLI and the effectiveness of interactive means for learning about location privacy. The main limitation of this research activity is its vagueness: The design and basic functionality of the used learning tool depend on the results of Study 2 and are therefore still uncertain.

Timeline


2020
2021
2022
2023
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Jun
Proposal
Study 1.1: Elicit status quo of location privacy in literature
Study 1.2: Analysis of commercial location based services
Study 2: Explorative deployment study with mobile learning tool
Study 3: Extended learning tool study
Wrap up and composition of dissertation
Proposal
Literature Research
Creation of conceptual model + collaborative writing of journal paper
Creation of app corpus and analysis scheme
Analysis of apps by two raters
Collaborative writing of conference paper
Conceptualization, iterative development and testing of mobile application
Preparations for study
Deployment study
Collaborative writing conference paper
Development learning tool
Study
Development learning tool
Study
Development learning tool
Study
Collaborative writing of journal paper
Buffer
Wrap up and composition of dissertation

References

[1] Almuhimedi H, Schaub F, Sadeh N, Adjerid I, Acquisti A, Gluck J, Cranor LF, Agarwal Y (2015) Your location has been shared 5,398 times! a field study on mobile app privacy nudging. In: Proceedings of the 33rd annual ACM conference on human factors in computing systems, pp 787–796

[2] Anthony D, Henderson T, Kotz D (2007) Privacy in location aware computing environments. IEEE Pervasive

[3] Ardagna CA, Cremonini M, Damiani E, Di Vimercati SDC, Samarati P (2007) Location privacy protection through obfuscation-based techniques. In: IFIP Annual Conference on Data and Applications Security and Privacy, Springer, pp 47–60

[4] 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 12(3-4):141–178

[5] Ataei M, Degbelo A, Kray C, Santos V (2018) Complying with privacy legislation: From legal text to implementation of privacy-aware location-based services. ISPRS international journal of geo-information 7(11):442

[6] Bargiotti L, Gielis I, Verdegem B, Breyne P, Pignatelli F, Smits P, Boguslawski R, et al (2016) Guidelines for public administrations on location privacy: European union location framework. Tech. rep., Joint Research Centre (Seville site)

[7] Barkhuus L (2004) Privacy in location-based services, concern vs. coolness. In: Workshop on Location System Privacy and Control at MobileHCI, Citeseer, vol 4

[8] Barkhuus L, Dey AK (2003) Location-based services for mobile telephony: a study of users' privacy concerns. In: Interact, Citeseer, vol 3, pp 702–712

[9] Benisch M, Kelley PG, Sadeh N, Cranor LF (2011) Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs. Personal and Ubiquitous Computing 15(7):679–694

[10] Beresford AR, Stajano F (2003) Location privacy in pervasive computing. IEEE Pervasive computing 2(1):46–55

[11] Bettini C (2018) Privacy protection in location-based services: a survey. In: Handbook of Mobile Data Privacy, Springer, pp 73–96

[12] Boutet A, Gambs S (2019) Inspect what your location history reveals about you: Raising user awareness on privacy threats associated with disclosing his location data. In: Proceedings of the 28th ACM International Conference on Information and Knowledge Management, pp 2861–2864

[13] Burghardt T, Buchmann E, Müller J, Böhm K (2009) Understanding user preferences and awareness: Privacy mechanisms in location-based services. In: OTM Confederated International Conferences" On the Move to Meaningful Internet Systems", Springer, pp 304–321

[14] Chatzikokolakis K, ElSalamouny E, Palamidessi C, Pazii A (2017) Methods for location privacy: A comparative overview. Foundations and Trends® in Privacy and Security 1(4):199–257

[15] Cohen J (1968) Weighted kappa: nominal scale agreement provision for scaled disagreement or partial credit. Psychological bulletin 70(4):213

[16] Cottrill CD, et al (2015) Location privacy preferences: A survey-based analysis of consumer awareness, trade-off and decision-making. Transportation Research Part C: Emerging Technologies 56:132–148

[17] Couture S, Toupin S (2017) What does the concept of'sovereignty'mean in digital, network and technological sovereignty? In: GigaNet: Global Internet Governance Academic Network, Annual Symposium

[18] Cvrcek D, Kumpost M, Matyas V, Danezis G (2006) A study on the value of location privacy. In: Proceedings of the 5th ACM workshop on Privacy in electronic society, pp 109–118

[19] Di Geronimo L, Braz L, Fregnan E, Palomba F, Bacchelli A (2020) Ui dark patterns and where to find them: a study on mobile applications and user perception. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, pp 1–14

[20] Drakonakis K, Ilia P, Ioannidis S, Polakis J (2019) Please forget where i was last summer: The privacy risks of public location (meta) data. arXiv preprint arXiv:190100897

[21] Görlach A, Heinemann A, Terpstra WW (2005) Survey on location privacy in pervasive computing. In: Privacy, security and trust within the context of pervasive computing, Springer, pp 23–34

[22] Gruteser M, Grunwald D (2003) Anonymous usage of location-based services through spatial and temporal cloaking. In: Proceedings of the 1st international conference on Mobile systems, applications and services, pp 31–42

[23] Kar B, Crowsey RC, Zale JJ (2013) The myth of location privacy in the united states: Surveyed attitude versus current practices. The Professional Geographer 65(1):47–64

[24] Kido H, Yanagisawa Y, Satoh T (2005) An anonymous communication technique using dummies for location-based services. In: ICPS'05. Proceedings. International Conference on Pervasive Services, 2005., IEEE, pp 88–97

[25] Krishen AS, Raschke RL, Close AG, Kachroo P (2017) A power-responsibility equilibrium framework for fairness: Understanding consumers' implicit privacy concerns for location-based services. Journal of Business Research 73:20–29

[26] Krumm J (2009) A survey of computational location privacy. Personal and Ubiquitous Computing 13(6):391–399

[27] Li N, Chava V, Li L (2017) A labware for educating location privacy protection in location-based services. Journal of Computing Sciences in Colleges 32(4):40–48
[28] Lin J, Amini S, Hong JI, Sadeh N, Lindqvist J, Zhang J (2012) Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In: Proceedings of the 2012 ACM conference on ubiquitous computing, pp 501–510
[29] Misterek F (2017) Digitale souveränität: Technikutopien und gestaltungsansprüche demokratischer politik. Tech. rep., MPIfG Discussion Paper
[30] Park YJ, Jang SM (2014) Understanding privacy knowledge and skill in mobile communication. Computers in Human Behavior 38:296–303
[31] Poikela M, Toch E (2017) Understanding the valuation of location privacy: a crowdsourcing-based approach. In: Proceedings of the 50th Hawaii International Conference on System Sciences
[32] Riederer C, Echickson D, Huang S, Chaintreau A (2016) Findyou: A personal location privacy auditing tool. In: Proceedings of the 25th International Conference Companion on World Wide Web, pp 243–246
[33] Toch E, Cranshaw J, Drielsma PH, Tsai JY, Kelley PG, Springfield J, Cranor L, Hong J, Sadeh N (2010) Empirical models of privacy in location sharing. In: Proceedings of the 12th ACM international conference on Ubiquitous computing, pp 129–138
[34] Tsohou A, Kosta E (2017) Enabling valid informed consent for location tracking through privacy awareness of users: A process theory. Computer Law & Security Review 33(4):434–457
[35] Wernke M, Skvortsov P, Dürr F, Rothermel K (2014) A classification of location privacy attacks and approaches. Personal and ubiquitous computing 18(1):163–175
[36] Wood A, Altman M, Bembenek A, Bun M, Gaboardi M, Honaker J, Nissim K, O'Brien DR, Steinke T, Vadhan S (2018) Differential privacy: A primer for a non-technical audience. Vand J Ent & Tech L 21:209
[37] Yun H, Han D, Lee CC (2013) Understanding the use of location-based service applications: do privacy concerns matter? Journal of Electronic Commerce Research 14(3):215