Location Privacy Revisited: Factors of Privacy Decisions

Benjamin Henne
Distributed Computing & Security Group
Leibniz Universität Hannover
Schloßwender Str. 5
30159 Hannover, Germany
henne@dcsec.uni-hannover.de

Matthew Smith
Distributed Computing & Security Group
Leibniz Universität Hannover
Schloßwender Str. 5
30159 Hannover, Germany
smith@dcsec.uni-hannover.de

Marian Harbach
Distributed Computing & Security Group
Leibniz Universität Hannover
Schloßwender Str. 5
30159 Hannover, Germany
harbach@dcsec.uni-hannover.de

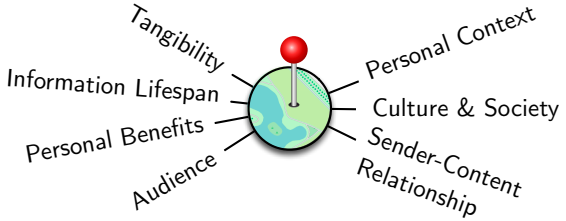

Figure 1: Seven factors of location privacy decisions

CHI 2013 Extended Abstracts, April 27–May 2, 2013, Paris, France.
ACM 978-1-4503-1952-2/13/04.

Abstract
The privacy problems associated with disclosing location information have repeatedly been the subject of research during the past decade. Yet, only the increasing adoption of smartphones today unveils real world implications, since a large number of users currently use location-based services and GPS-enabled devices for a multitude of purposes. Recently, research suggested that location privacy is not a relevant problem for today's users. However, a study we conducted indicates that it might be too early to call off investigations of location privacy: In a survey of 414 users on online media sharing behavior, we found that location was rated as the type of photo metadata that poses the highest risk to privacy. Therefore, we revisit the discussion on location privacy in this paper and propose factors that can explain the conflicting views.

Author Keywords
Location; Privacy; Location-based services; Human factors

ACM Classification Keywords
H.1.2 [**Models and Principles**]: User/Machine Systems—*Human Factors*.

General Terms
Human Factors, Security

Introduction

Location sharing and its privacy implications have a long history in HCI research. Additionally, many people's lives are increasingly permeated by smartphones and tablets, making this a relevant topic for a wide audience. Location-based services are used on a daily basis to get information on weather, a café in the vicinity, or to meet with friends. Overall, apps and smartphones have realized most of the usage scenarios predicted in previous work. While many aspects of location privacy have been discussed in the past decade, potential real world problems have not appeared until recently. For example, in December 2012, the whereabouts of John McAfee, who was in hiding at that time, were disclosed by a photo taken with a journalist's smartphone[1], because GPS coordinates automatically added to the image's metadata were not removed before publication. However, latest research [3, 5] suggests that location privacy is not a severe privacy problem for most users, since many other problems are worse and research should focus on those.

We conducted a study with results that suggest otherwise: In a survey of 414 users on photo sharing and awareness on the social Web, our participants indicated photos with location information in the metadata as the most severe privacy problem possible to occur when sharing media online. In order to put these results into perspective, we aim to revisit the long lasting discussion on location privacy and investigate the state of affairs given the current prevalence of smartphones. In this paper, we present the following contributions to the location privacy discussion in the HCI community:

- We dispute the statement that location privacy is currently not a relevant problem for users.
- We analyze previous work on location privacy and relate these results to the findings of our survey.
- We identify a set of factors that we believe influence the perception of location privacy and hence users' privacy decisions.

[1] http://gizmodo.com/5965295/vice-magazine-just-accidentally-revealed-where-john-mcafee-is-hiding

Related Work

There is a considerable history of related work on location privacy. Since the advent of GPS-enabled devices and camera phones, researchers have investigated the implications of adding location to shared data. In particular, Consolvo et al. [2] presented a first formative study on location privacy and disclosure in 2005. They found that the relationship towards the requester of location information and the purpose of the request informed the users' decisions. Subsequently, Ahern et al. [1] presented a study on sharing photos with location data using mobile phones. Their results indicate that the disclosure of a photo's location causes concerns, especially with parents, while other users appear entirely unconcerned. They also note that users only suppressed location information in 2 % of uploaded photos. However, they were only able to use cell-tower-based location information on a zip code-level at the time of writing their paper.

In more recent publications, authors doubt that location disclosure still raises much concern with today's smartphone users in comparison with the beginning of the mobile era. Krumm [4] summarizes different results showing that people do not seem to care about location privacy: For instance, in several studies, participants were ready to share weeks and months of location traces for a small amount of money and only one fifth objected to commercial use of that data. In the "very-upset-ranking" of 99 risks associated with different smartphone

Survey Design

Preparation: We invited 1,418 subscribers of a mailing list at our university to a study on photo sharing behavior. On completion, participants could enter a raffle for two $ 60 Amazon vouchers.

Design: Online survey with 28 rating and multiple choice questions on metadata, sharing behavior and awareness of potential problems.

Participants: 414 complete and valid answers; 53.9 % male and 46.1 % female; university students from computer to social science; 22.2 % indicated high or very high technical expertise; average age 23 ± 4 years; Westin's privacy segmentation index: 91.8 % pragmatists, 6.0 % fundamentalists, 2.2 % unconcerned.

permissions of Porter Felt et al. [5], the participants ranked location-related risks in the bottom half and the actual location was ranked second-lowest out of eleven data types.

In another paper, Fisher et al. [3] show that some users are aware of location and privacy implications: in their study, iOS users selectively granted apps access to location information. Their participants did not disallow location-use in general, seemingly making decisions based on the expected value of each app.

Survey of Photo Sharing and Locations

We conducted an online survey to investigate user behavior and perceptions of photo sharing, metadata and tradeoffs regarding privacy (cf. sidebar). Photo sharing is one of the major activities of social media users. Services such as Instagram currently have more than 100 million users with more than 200 pictures being uploaded per second at times[2]. In our survey, we also captured attitudes towards location.

One aim of our survey was to assess the users' view of the privacy implications of different pieces of photo metadata and how severe users estimate a possible privacy violation caused by the disclosure of such data to be. We asked our participants to rate the possible privacy impact of several kinds of metadata in shared media (cf. Table 1) added either by themselves (a) or by others (b) on a 7-point scale from 1 = *very low* to 7 = *very high*. Furthermore, we asked the participants about their general privacy perceptions concerning different kinds of metadata on a 7-point scale from 1 = *completely public* to 7 = *completely private*. The answers are shown in Figure 2.

[2] http://techcrunch.com/2012/11/23/instagram-thanksgiving/

In all three questions (cf. Listing 1), exact location (coordinates from GPS or Wi-Fi tracking, postal addresses) is found to be the top concern, while broad location (city, postal code, region) is perceived to have at least medium impact on privacy. These results are in conflict with the recent related work presented above. Porter Felt et al. [5] as well as Krumm [4] presented studies showing that participants had little concerns about disclosing location data.

metadata added by with impact to	(a) participant others		(b) others participant	
	mean	*sd*	*mean*	*sd*
headline, description, tags***	2.94	1.66	3.23	1.75
date & time of creation^{ns}	3.63	1.70	3.59	1.67
photographer's name**	3.49	1.79	3.28	1.83
depicted people's names***	5.08	1.70	4.76	1.87
broad location (city, region)^{ns}	3.95	1.62	3.90	1.74
exact location (address, GPS)*	5.31	1.68	5.17	1.75

significance of Wilcoxon signed rank test of (a) and (b): $^{***}: p < .001$, $^{**}: .001 \leq p < .01$, $^{*}: .01 \leq p < .05$, $^{ns}: p \geq .05$

Table 1: Participants' estimation on the impact of metadata

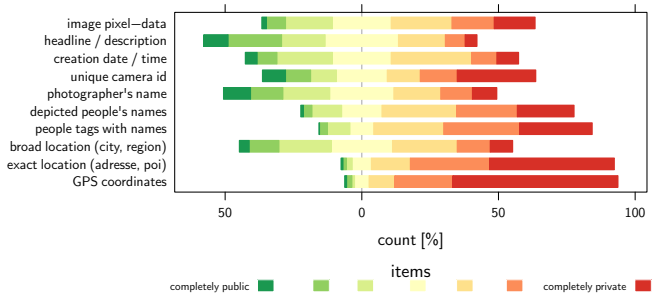

Figure 2: Privacy perceptions of different photo metadata

Additionally, our survey assessed the influence of the audience when disclosing location data: Users were asked

photo audience	feeling *mean* (*sd*)	top 2 %
friends	2.24 (1.5)	3.9
indirect friends	3.51 (1.7)	14.3
strangers	5.16 (1.8)	51.9
hosting service	5.23 (1.9)	54.1
privacy service	5.28 (1.9)	57.2

Table 2: Participants' feeling if others get to see a photo of them that includes location data

q23: Rate the possible privacy impact to others if you add these types of metadata to photos that you share. (7-point scale: *very low* to *very high*)

q24: Rate the possible privacy impact to yourself if others add these types of metadata to photos that they share. (7-point scale: *very low* to *very high*)

q29: How do you feel about the privacy of this photo metadata? (7-point scale: *completely public* to *completely private*)

Listing 1: Survey excerpt

to rate how they would feel if people got to see a photo of them that includes location information, using a 7-point scale from 1 = *very unconcerned* to 7 = *very concerned* with 4 as *neutral*. Results (cf. Table 2) again contradict previous work: When sharing a photo including location data with friends or friends of friends, participants state to be more or less unconcerned. They were more concerned in the case of strangers. However, when it comes to servers, for instance the service provider that hosts a shared photo, people stated to be even more concerned. This also conflicts with the results of Porter Felt et al. [5], who found that people were less concerned about disclosing location to servers than to friends, the public or advertisers.

Discussion

The results of our study show that location information still raises concerns for users. The conflicting results of recent related work and our study indicate that differences in participants or study design influence the privacy implications of disclosing location data: First, the participants of our survey and correspondingly their privacy perceptions may differ from prior studies. Second, the other recent studies on location privacy addressed different contexts of using location information: while some focused on smartphone apps [5, 3] or giving away comprehensive location traces [4], our study and Ahern et al. [1] focused on sharing media. There were also differences in the investigated scenarios: most of the studies cited in Krumm's overview [4] used hypothetical location-based services or asked for data in the context of research. The study of Port Felt et al. mainly compared the impact of location disclosure with other risks on smartphones, such as losing all contacts or photos on the phone, while Ahern et al. and our study mainly used location and photo sharing as a basis.

These differences in research design and results suggest a set of factors that influence the perception of location privacy and hence users' privacy decisions. In the following, we provide an initial discussion of seven potential factors (cf. Figure 1), which we aim to explore further in future work. We believe that these factors can serve as a basis for future privacy research and allow the HCI community to gain an increased understanding of the role of location privacy in modern information systems.

Information Lifespan A central difference between previous studies on location privacy and ours is the medium which the location information is conveyed with. A set of locations shared with a location-based service to find restaurants or get the local weather does not cause great concern for users according to the related work, while, according to our results, a set of photos with location tags discoverable on the Internet does. A possible explanation for this difference is the perceived lifespan of shared information: we believe that there is a difference between data that is only accessible at a particular service like Foursquare, or a location that is shared, stored and duplicated with another piece of information. While the information is potentially public in both cases, the features of modern search engines for example can cause users to perceive public photos to be more persistent and hence more easily discoverable in the future.

Audience Prior research shows that people may perceive privacy threats by nearly any other person, i. e. from within or outside of their social groups. Additionally, known service providers like Facebook as well as more anonymous services like a weather forecast service are part of the audience. The audience and the implied trust influence the privacy concerns and hence the decision on whether or not to disclose location information. The

upset-ranking for location disclosure [5] strongly depended on audience: While 72 % of respondents stated to be very upset if a location is shared publicly, only about 60 % were concerned about disclosure to friends and advertisers and 30 % about disclosure to a service provider. Similarly, our participants were less concerned about disclosing photos with location information to friends, but were concerned about disclosure to strangers and especially concerned about disclosure to a service on the Web (cf. above). There also is a notable difference in these two result sets: While our participants were most concerned about service providers, those caused the least concern in the results of Porter Felt et al. We believe that this difference can be attributed to the additional factors discussed in this work.

Personal Benefits Personal benefits are another possible factor for the perceived privacy of location data: people weigh the benefits of disclosing their location against the potential privacy impact when deciding for or against location disclosure. As recently shown by Fisher et al. [3], iOS users chose which apps to allow to use their location information based on perceived benefits. Their participants more frequently allowed apps such as map services or Foursquare the use of their current location, but hesitated to authorize apps like music services. While the perceived personal benefit may not influence the perception of privacy directly, it can influence the ultimate decision about location privacy.

Sender-Content Relationship We believe that the relationship between who shares information about whom also influences the privacy perception of that piece of information. If someone is able to publish location information about someone else without asking that person first, this pattern of sharing can cause more harm to a person's privacy than information consciously shared by that person herself. Our study addressed differences of such scenarios and their impact on privacy perceptions: We collected severity ratings for privacy violations caused by metadata added to photos being shared by others as well as for metadata in photos shared by the user. We found that users often assigned more privacy impact to their own sharing behavior than to the behavior of others (cf. Table 1).

Culture and Society Another potential factor influencing the perception of location privacy is the difference of attitudes towards privacy as introduced by differences in culture and society. Wang et al. [6] for instance showed that privacy attitudes differed between American, Chinese and Indian users when sharing city- or street-level location in social network services. While the participants of most prior studies were recruited in the U.S., the participants of our study were recruited in Germany. The cultures of America and Germany may in many cases differ less than those compared by Wang et al., but Germans are commonly assumed to be more sensitive concerning their privacy.

Personal Context Users' experiences with location information may also influence the perception of location privacy: Users that are used to work with location information may also care less about the privacy implications. The results of our survey suggest such a connection: the more participants add location information to their photos, the less they are concerned about a possible privacy impact through location information (Spearman's $\rho = -0.234$, $p < .001$). Users' awareness of disclosed information may also influence privacy concerns: In our survey, 29 % of those 253 participants that indicated to know what metadata is stated not to know what information is stored in the

photos they share. In the case of John McAfee and the published photo, someone did not remember or even did not know that the journalist's smartphone automatically added a location to the photo and hence unknowingly distributed the coordinates to all readers of the article. Additionally, if location is used within contexts such as photos or micro-blog posts, the content of a shared picture or text as well as the user's personal situation is known to influence the privacy perceptions: In the study of Ahern et al. [1], parents were especially concerned about sharing location information for pictures showing their children.

Tangibility Based on the differences between our and previous results, we suspect that the need for privacy of location information is also influenced by the tangibility of the sharing medium. For instance, our survey was based on a scenario of sharing photos on the Web. In this case, location is at least connected to the visual contents of a picture and possibly to additional metadata. Digital photos are indeed not touchable, but still much more concrete for the participants than a string of GPS coordinates recorded by a service. The more recent studies on location privacy mainly deal with location in the context of location-based services, pro-active publication of locations, or the misuse of location permissions by smartphone applications. In all these cases, location and where or how that information is stored are less tangible for users. To the best of our knowledge, no previous work compared users' perceptions of location privacy with respect to different types of sharing channels.

Conclusion

In this work, we argued for the importance of revisiting location privacy. Results of a survey with 414 participants on photo sharing and metadata were in conflict with previous investigations and showed that current users are concerned about the impact of unwanted disclosure of location data. While there may be other important privacy issues to be investigated in modern communication platforms as postulated by Porter Felt et al. [5], our results indicate that there is more to location privacy than has been explored by available research. We proposed a set of seven factors that we believe have an influence on the perceptions of location privacy of users and their ultimate privacy decisions. In our next steps, we plan to investigate the relative impact of each factor as well as provide a more comprehensive and conclusive picture of location privacy in modern communication systems.

References

[1] Ahern, S., Eckles, D., Good, N., King, S., Naaman, M., and Nair, R. Over-exposed? Privacy Patterns And Considerations In Online And Mobile Photo Sharing. In *Proc. CHI*, ACM (2007), 357–366.

[2] Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., and Powledge, P. Location Disclosure to Social Relations: Why, When, & What People Want to Share . In *Proc. CHI*, ACM (2005), 81–90.

[3] Fisher, D., Dorner, L., and Wagner, D. Location Privacy: User Behavior In The Field. In *Proc. SPSM*, ACM (2012), 51–56.

[4] Krumm, J. A Survey Of Computational Location Privacy. *Personal and Ubiquitous Computing 13*, 6 (2009), 391 – 399.

[5] Porter Felt, A., Egelman, S., and Wagner, D. I've Got 99 Problems, But Vibration Ain't One: A Survey Of Smartphone Users' Concerns. In *Proc. SPSM*, ACM (2012), 33–44.

[6] Wang, Y., Norice, G., and Cranor, L. Who Is Concerned About What? A Study Of American, Chinese and Indian Users' Privacy Concerns On Social Network Sites. In *Proc. TRUST*, Springer (2011), 146–153.