future internet

MDPI

Review

Toward Addressing Location Privacy Issues: New Affiliations with Social and Location Attributes

Katerina Vgena [1,*], Angeliki Kitsiou [1], Christos Kalloniatis [1], Dimitris Kavroudakis [2] and Stefanos Gritzalis [3]

[1] Privacy Engineering and Social Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, GR 81100 Lesvos, Greece; a.kitsiou@aegean.gr (A.K.); chkallon@aegean.gr (C.K.)
[2] Department of Geography, University of the Aegean, GR 81100 Lesvos, Greece; dimitrisk@aegean.gr
[3] Department of Digital Systems, University of Piraeus, GR 18534 Piraeus, Greece; sgritz@unipi.gr
* Correspondence: kvgena@aegean.gr

Received: 23 September 2019; Accepted: 30 October 2019; Published: 1 November 2019

Abstract: Nowadays, location-sharing applications (LSA) within social media enable users to share their location information at different levels of precision. Users on their side are willing to disclose this kind of information in order to represent themselves in a socially acceptable online way. However, they express privacy concerns regarding potential malware location-sharing applications, since users' geolocation information can provide affiliations with their social identity attributes that enable the specification of their behavioral normativity, leading to sensitive information disclosure and privacy leaks. This paper, after a systematic review on previous social and privacy location research, explores the overlapping of these fields in identifying users' social attributes through examining location attributes while online, and proposes a targeted set of location privacy attributes related to users' socio-spatial characteristics within social media.

Keywords: social and spatial characteristics; geolocation information; privacy concerns

1. Introduction

Social media's popularity and the availability of sharing one's location instantly in such detail raises questions in handling socio-spatial information [1–3]. On the one hand, privacy issues are thought to be of prior importance while users interact in social media applications. According to [4], "Privacy is regarded as a fundamental human right, internationally recognized in Article 12 of the UN Universal Declaration of Human Rights" (p. 3). Under that spectrum, users' privacy concerns, which are triggered by malicious users, seem to engage social software engineering researchers in a vital dialogue aiming to design appropriate solutions to address those needs.

On the other hand, although hardly a day goes without users being perplexed or discussing their privacy concerns, it seems that their insecurities do not prevent them from possessing accounts and using location-sharing applications while sharing social and location information in all levels of granularity [5]. The incompatibility between users' perceptions and their everyday practice is known as the privacy paradox [6]. Users are willing to unveil parts of their intimacy, turning them into entertainment content that will be consumed as extimacy (public content that is shared and uploaded online) for engaging in social media encounters [7].

Users tend to overcome their concerns while online to take advantage of social media services disclosing information such as their age, gender, or other personal information [8]. This type of information, which is part of their social identity, can be analyzed through the social identity theory [2,9,10]. More precisely, the main characteristics of social identity namely, multiplicity,

permeability, and overlapping have already been meticulously analyzed [7]. However, social media representation of location information provides space for further analysis on social digital identities' main characteristics. In that way, additional notions closely related to users' location information are introduced as new variables to our study. Users' location information can trigger the revealing of their identity, even though users do not always feel that their information is going to be used in a suspicious way for the purposes of this paper [1,4,9]. Therefore, this type of information can be "treated as one type of personal information, like age, gender, or address" (p. 7) [4].

In this regard, the aim of this study is to conduct a systematic review broadening the understanding of the way that users' digital identities are affected by the disclosure of geolocation information, leading to location privacy threats. In particular, the review focuses on identifying potential location privacy concerns and threats that are generated by social and location information disclosure. The study, based on social identity and location privacy theories, through an interdisciplinary approach, attempts to examine users' social and location information within the context of sensitive personal information [4]. By providing new affiliations between users' social and location attributes, a set of location privacy attributes related to users' socio-spatial characteristics is targeted and identified, providing groundwork for the development of appropriate methodologies to address location privacy issues.

The rest of the paper is structured as follows. In Section 2, we analyze our methodology for completing the review and we discuss the research questions under study. After that, we present the results of our study, while discussing geosocial networks, digital identity attributes, and geolocation information in relation to location privacy concerns and threats; we also summarize the attributes of geolocation information and digital identities in order to identify location privacy issues through geolocation and social attributes. Section 4 presents the discussion of our paper after conducting the systematic review. This section introduces the attributes of location privacy that are related to users' socio-spatial characteristics. Future directions of research are discussed in the last section of our paper along with the conclusion and the limitations of our work.

2. Materials and Methods

We have screened a total number of 1,626,800 papers in our review. The purpose of this study is to employ a systematic mapping that identifies specific users' socio-spatial characteristics in addressing privacy concerns and potential threats. Existing research work on the field will assist in identifying opportunities and gaps for future research. In order to carry out the systematic review, we utilized guidelines and research recommendations based on the conceptual model of the PRISMA 2009 flow diagram in our methodology [11].

The study was conducted from the second half of 2018 to the first trimester of 2019 and it covers papers from 2001 to 2018 publications about the socio-spatial characteristics of users, as well as the spatial and the social privacy concerns of users in online social networks. More precisely, the review was conducted through database searching in google scholar, Scopus, IEEE, ScienceDirect, and Semantic Scholar.

The database searching was initiated by inserting the aforementioned research words and synonyms, which were categorized in four main categories—privacy threats/concerns/risks (approximately 560,000 papers), location and proximity services, location-based services and applications (approximately 401,500 papers), privacy location/geolocation privacy, privacy requirements (approximately 35,300 papers), and identity location, identity, and privacy, social identity/digital identity (approximately 630,000 papers)—in all five search engines.

The result was concluded after arriving at a significant number of articles that should be narrowed down not only in terms of duplicate articles but also in terms of combining both social identity and location privacy theories in an interdisciplinary way. In that way, we narrowed down the results of the search to 82 papers in the first phase of the selection of our papers. Table 1 presents the criteria applied during the exclusion process.

Table 1. Exclusion Criteria (first phase).

Exclusion Criteria
1. Studies dealing only with geolocation privacy risks 2. Studies dealing only with personal identity in social media

After proceeding with that necessary step, we have also applied a second phase of exclusion criteria for choosing the reviewed papers. Table 2 summarizes the exclusion criteria for the second phase. After that phase, we ended up with 36 research papers for conducting our review.

Table 2. Exclusion Criteria (second phase).

Exclusion Criteria
1. Studies that were not accessible in full-text 2. Studies that were not written in English

A Prisma 2009 flow diagram was also utilized as a means to visually represent the reviewing process of our paper. Figure 1 represents an adjustment of the proposed visualization of this process:

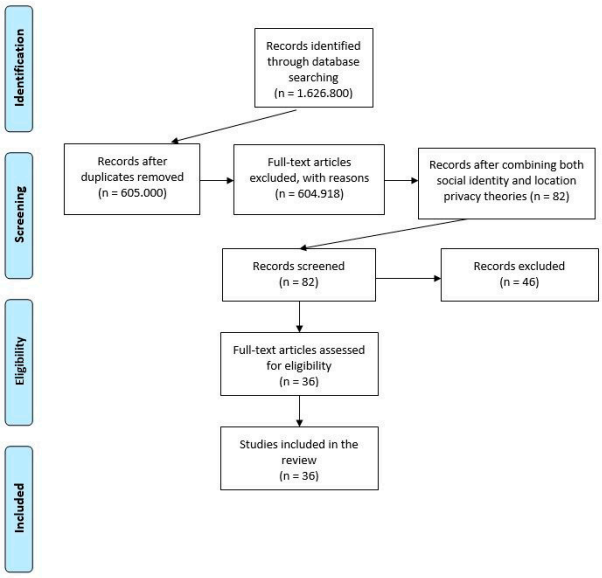

Figure 1. Methodology processes under Prisma 2009 flow diagram.

As the primary concern of this paper is to specify proper attributes for identifying users' geospatial and social characteristics before designing socially aware information systems, the reviewed papers were focusing on characteristics of social or digital identity, and thus face and geospatial characteristics. Previous literature [1] suggests that location privacy is not just linked to GPS coordinates (x, y) or representations of names, but most importantly, it includes user's identity, position/place in the world, and time of the action. At this point, the analogy among identity (who), position (where), and time (when) is rather obvious. Going a step further and drawing on that theory [1] while reviewing the aforementioned papers, we concluded that except for these three very important attributes of location information, it is important to add a fourth one: the attribute of the activity, or in other words, what is the action or what is happening (what). Thus, our study identified four attributes of location information, namely the attributes of who, what, when, and where before moving to the research questions of the study.

Based on the aforementioned characteristics, the following research questions were also formulated, as shown in Table 3.

Table 3. Research Questions of the Review.

Research Questions of the Review
RQ1a: Does the interrelation of users' geospatial and social characteristics trigger additional privacy concerns and threats? RQ1b: What are the major scales measuring socio-spatial location privacy concerns?

Under this spectrum, we proceeded in saving and tagging each paper to Zotero so as to be able to list all possible combinations of geolocation attributes—who, what, when, and where—to address our research questions. The aforementioned categorization enables us to sort papers that dealt both with geolocation information and social identity at the same time. That step was important for our analysis, as it combined both the "who" and "where" attributes, which address the RQ1a: Does the interrelation of users' geospatial and social characteristics trigger additional privacy concerns and threats?" In other words, we can examine how we can apply the aforementioned variables in identifying users' social identity via their habits. More precisely, Table 4 lists all possible combinations of papers using Zotero tagging.

Table 4. Possible Combinations of Papers Using Zotero Tagging.

Possible Combinations of Papers Using Zotero Tagging	
One Tag	who where when what
Two Tags	who, what who, when who, where what, when what, where when, where
Three Tags	who, what, when what, when, where who, when, where who, what, where
Four Tags	who, what, when, where

Table 5 summarizes the steps followed for choosing and categorizing the relevant set of research papers in the field under study. The below-mentioned steps were followed:

Table 5. Steps of the Systematic Review.

Steps of Categorizing the Reviewed Papers
1. Define the research terms according to the research questions—words and synonyms—and categorize them in four main categories: privacy threats/concerns/risks; location and proximity services, location-based services and applications; privacy location/geolocation privacy and privacy requirements; and identity location, identity and privacy, and social identity/digital identity.
2. Search academic papers at google scholar, Scopus, IEEE, ScienceDirect, and Semantic Scholar.
3. Save all papers to Zotero and tag them according to the geolocation attributes of who, what, when, and where.
4. List the articles in an excel file, with all possible combinations with one tag (who, what, when, where), two tags (who, what), (who, when), (who, where), (what, when), (what, where), (when, where), three tags (who, what, when), (what, when, where), (who, when, where), (who, what, where), and four tags (who, what, when, where) so as to proceed in categorizing papers.

While defining the research terms according to which we launched the research in the aforementioned academic resources, we identified approximately 560,000 papers for the category privacy threats/concerns/risks, approximately 401,500 papers papers for the category location and proximity services, location-based services, and applications, approximately 35,300 papers for the category privacy location/geolocation privacy and privacy requirements; and approximately 630,000 papers for the category identity location, identity and privacy, and social identity/digital identity.

After completing the screening process and conducting our systematic review, we were provided with a list of all-important abbreviations used in the reviewed papers. Table 6 presents the summary of important abbreviations used in the aforementioned papers:

Table 6. Summary of Important Abbreviations Used in the Reviewed Papers.

Location Privacy	Social Identity
GPS	Global Positioning System
MSN	Mobile Social Network
LBS	Location-Based Service
LBA	Location-Based Application
LSA	Location-Sharing Applications
PIR	Private Information Retrieval
LPPM	location privacy preservation mechanism
OSNs	Online Social Networks
mOSNs	mobile Online Social Networks
GeoSNs	Geo-Social Networks
LBSNs	Location-Based Social Networking services
LBRTD	Location-Based Real-Time Dating app
PETs	Privacy Enhancing Technologies
TPLBSP	Third Party Location-Based Service Provider
SI	Social Identity

3. Results

In this systematic review, we have included 36 papers in an attempt to focus on the papers that covered users' geospatial and social characteristics and at the same time identify location privacy issues. For the purposes of our study, it was important to proceed with a categorization of the papers that to the best of our knowledge have already discussed geolocation and social identity issues. That was our primary goal when organizing the respective subsections, namely geosocial networks; users' identity through geolocation information; identifying users' identity—location privacy concerns and identifying users' identity—threats; attributes of geolocation information and digital identities; location privacy issues through geolocation information, and digital identities attributes. More specifically, the papers have been divided into the following six categories: namely, papers that refer to geosocial networks, papers discussing the representation of user's identity in geosocial networks through geolocation information, papers that examine users' concerns and privacy issues, and papers focusing on threats that may arise due to the information leak of a user's location. After that, we also focus on matching attributes of geolocation information to attributes of social identity, and we discuss the location privacy issues that arise due to geolocation information or digital identities attributes disclosure.

In particular, this categorization of the papers reflects the rationale of our study. First and foremost, it was important to gain a better understanding of geosocial networks, which is considered to be a milestone in deepening our study. That is because building upon the way that users tend to use social media and at the same time represent themselves while online may raise questions about their online representation, which apart from social characteristics, utilizes geospatial descriptions. On the second category we focus on geospatial landmarks that frequently aim to add social characteristics to users profiles, i.e., social media users may state the name of their institution not only to describe their place in the world but rather represent themselves as members of academia or alumni of a higher institution in order to offer their online representations an educational status [12]. Deepening our understanding

of geosocial networks and how users represent themselves online, we move to the third category, as we cannot disregard users' privacy concerns. It is worth mentioning that although users seem to express their concerns about potential information leaks and malicious users, they do not hesitate to use geosocial networks or geotag themselves [6,7]. That incompatibility, which has already caught our attention in the introduction, motivates us to shed light upon the fourth category of papers in our study, which aims to identify possible threats (malware or private profit) that could harm users' online activity. The fifth category of papers matches geolocation attributes to attributes of social identity, while the sixth category discusses location privacy issues, which should be discussed due to the leaks related to geolocation information or digital identities attributes.

3.1. Geosocial Networks

Logging into geosocial networks seems to be an integral part of users' online practice. The rise and popularity of geosocial applications are likely to represent a "primary source of information about our surroundings" (p. 1) according to [13]. Puttaswamy et al. underline the shortage of privacy mechanisms indicating probable threats due to leaks of a user's activities enabling tracking or predicting habitual actions. After summarizing the three approaches according to which users' privacy is being conducted, namely, "(1) introducing uncertainty or error into location information, (2) relying on trusted servers or intermediaries to apply anonymization to user identities and private information, and (3) relying on heavy-weight cryptographic or private information retrieval (PIR) techniques" (p. 1), the study proposes the LocX, which is a new approach that despite utilizing exact accuracy as far as location information is concerned, protects users' privacy in location-based social applications (LBSAs) through encrypting users' location information so that only friends are able to decrypt them. Defining users' habits may provide enough information for tracking their normativity, which can prove to be a powerful means in making assumptions for users' upcoming actions and choices.

Geosocial networks are categorized by [14] into three privacy aspects—location privacy, absence privacy, and co-location privacy—in a way to address those concerns while discussing unresolved private challenges. Ruiz Vicente, Freni, Bettini, and Jensen define location privacy as "the sensitivity of the association between a user's identity and the user's location, be it the user's past, current, or anticipated future locations" (p. 2). Location privacy can reveal sensitive information, as a potential leak in absence privacy can signify an unattended place that is vulnerable to theft. Location information can also reveal information about potential relationships among users, due to the frequency they meet, and thus can prove to be quite important. Another aspect worth mentioning is co-location privacy, which is associated with co-location events and is frequently enjoyed, provided that users' identity is not linked to their co-location information. Spatio-temporal information may constitute a threat via re-identification through location or the release of sensitive location information. In that way, two possible solutions offered by this paper are to utilize spatial and temporal cloaking and encryption. However, it is argued that the aforementioned privacy-aware solutions are addressing only a certain subcategory of proximity-based services. Re-identification and tracking users' normativity when combining spatial and temporal information creates powerful affiliations on both users' past, current, or future habits in a way that is descriptive enough to raise location privacy concerns.

3.2. Users' Identity through Geolocation Information

The papers included in this category discuss how geolocation information is descriptive enough to provide specific information about users' identity through location infuriation.

Location-sharing applications (LSAs) as a part of location-based services support current location sharing among users. Tang, Lin, Hong, Siewiorek, and Sadeh in [15] take a closer look at the way that people share their geolocation information, using one-to-one or one-to-many sharing. In addition, this paper focuses on the difference of revealing a user's location based on the purpose, meaning for purpose-driven or social-driven purpose. The study focuses on the social-driven purpose and concludes that "social-driven location sharing favored semantic location names, blurring of location

information, and using location information to attract attention and boost self-presentation" (p. 10). The study was carried out on a limited number of participants for a limited period of time, while participants were all members of the academic community. That is, users tend to disclose their location information in a way that boosts their social status in order to catch other users 'attention. The next two articles can serve our purpose as examples of how users utilize location-aware services to represent themselves, adding desirable characteristics to their identities.

Bao, Zheng, and Mokbel suggest a location recommender system that is constituted of offline modeling (social knowledge learning and personal preference discovery), and online recommendation (preference aware candidate selection and location rating calculation) [16]. This paper investigates users' location histories in order to understand their preferences while traveling to a new city. The authors identify two main challenges that are linked to specifying users' preferences and defining a rating for a user's unknown place. Location recommendations match users' interests with nearby places by following specific requirements, namely user preferences, the current location of the user and the opinions of a location given by other users. The contribution of the study is proposing a location-based and preference-aware recommendation system that takes care of both user preferences, which are inferred by his/her location history, and social opinions, which are derived from local experts' location histories. For example, a user that identifies herself as "sommelier" has already provided information on her inclination from previous logs, and thus can acquire information on places of interest, e.g., wine bars, from other users with the same expertise.

Location-aware services are also employed in a number of dating applications, which are commonly used to match nearby individuals who are interested in meeting new partners. Birnholtz, Fitzpatrick, Handel, and Brubaker carry out a survey on how men who have sex with men (a term that refers to both people who identify themselves as gay and people who do not identify themselves as such) handle their identities and online information in order to represent themselves through Grindr. The representation is very condensed as far as language is concerned, as the focus is placed on users' images [12]. The language is of primary concern for users to identify themselves through a location. According to the study, except for neighborhoods, cities, and states, users tended to locate themselves through universities, as they function as landmarks carrying socio-economic or educational status. The study concludes that neighborhood level was used more often in larger cities, while users used the city-level identification either when they were present or while traveling.

According to Schwartz and Halegoua, [17] users' location information can be shared on social media applications in order to represent their identity. The term "spatial self" describes the representation of the user via geocoded online traces, adding information about his/her social sphere. Schwartz and Halegoua's term is defined as follows: "the spatial self is constituted from a bricolage of personal and collective, private and public meanings and narratives of place" (p. 13). Researchers conclude that in order to analyze geolocation information, it is important to combine both qualitative and quantitative methods. The paper analyzes information retrieved from Instagram, Facebook, and Foursquare. The notion of a spatial self underlines the importance of geolocation information in identifying users' identity while online in a way that draws on both social identity and geotagging theories, thus constituting one of the key aspects in our analysis.

Drawing on the notion of the spatial self from the aforementioned paper, we should also include Lefebvre's term of social body while discussing on the notion of space. In other words, the notion of space is thought to be constituted by "living bodies" [18]. Under this spectrum, social relationships along with the human body, which is perceived as a multi-sensor, are being investigated in the framework of spatial characteristics. In addition, Lefebvre also introduces the notion of everyday life in a way that incorporates "insights on time, multiple temporalities, and the time–body relationship" (p. 7) [18]. The author's comment on what time means for Lefebvre is also quite intriguing, as he underlines that "For Lefebvre, time was closely connected with space and apprehended in space, and both enjoyed the same ontological status" (p. 7) [18]. Lefebvre's analysis of the social body seems to

incorporate all four common attributes between the social and location attributes of our analysis, which should be in accordance with location privacy when designing privacy-aware information systems.

The next paper presents a new study based on graph metrics to analyze geosocial relationships among users by drawing on four popular online social networks. Scellato, Musolesi, Mascolo, and Latora introduce two metrics for geosocial networks: users' likelihood of exhibiting long (or short)-distance social interactions and the locality of social clusters [19]. Except for those metrics, the study also measures the tightness of each node. Social relationships are investigated in order to determine the role that distance can play. Close distance is associated with closer bonds when it comes to advertisements; however, it seems that this is not the case when it comes to new broadcasting, even in an online world where distance is not important for social relationships. Distance can play an important role in identifying relationships among users, as it is generally linked to closer bonds among them. However, distance should be associated with additional characteristics, as it is not possible to predict social relationships alone.

3.3. Identifying User's Identity—Location Privacy Concerns

Making assumptions about a user's identity through the disclosure of their geolocation information trigged a number of potential concerns. The following paper [20] proposes a new approach on handling location privacy concerns in services where users tend to share geolocation with other users ("friends" or "buddies") in a predetermined way in a geosocial network. Mascetti, Freni, Bettini, Wang, and Jajodia review previous work on this topic by mentioning Louis, Lester and Pierre, FriendLocator, and VicinityLocator, which are all different solutions in addressing privacy issues in proximity services. After carrying out a number of experiments, the authors evaluate the protocols according to a number of criteria. In other words, users share geolocation information among their friends while identifying each other as "friends". This absence of a more detailed way of distinguishing acquaintances from close friends opens a new discussion on who can have access to our location information. This question along with additional parameters is going to be addressed in the next two papers.

In [21], Snekkenes focuses on the "Who should have access to what location information under which circumstances?" question in a way to identify location, the identity of the user, time, and speed. The authors underline the need of the user to manage the accuracy settings of the abovementioned categories to address a user's needs or identity parameters. The paper identifies a number of concepts that need to be determined before moving to designing privacy policies, paying special attention to language.

In the next study [22], Consolvo, Smith, Matthews, LaMarca, Tabert, and Powledge wanted to investigate whether and what location information users would be willing to share with their acquaintances. The results of the study reveal that the most crucial factors for a user to disclose his/her location information included who was making the request, why the request was made in the first place, and what detail was useful to the acquaintance making the request. Having the aforementioned factors in mind, the participant would decide whether or not he/she would reveal the information requested. Other factors that played an important role included a user's activity and mood. More specifically, there were activities that users were more willing to reveal in relation to other activities. Mood was also important, as users tended to disclose their geolocation information when feeling depressed. Another important aspect was that participants did not opt for blurring their location information, as it was preferable for them to set social boundaries when the request was considered inappropriate, or because they thought that this level of information was useful for the requester. For example, when participants opted for less descriptive location information, it was not because they were not willing to share them, but because they thought that a more general statement would be more useful to the requester. The last finding of the study [22] makes us go a step further and draw an analogy to Grice's Cooperative Principle [23], according to which participants follow specific rules (maxims) in order to convey meaning. Grice's linguistic maxims seem to be in accordance with the study above as the maxim of quantity, according to which the speaker conveys only the amount of information

that is helpful to the listener, and the maxim of manner, according to which the speaker conveys only the clearest and briefest message possible and always expresses it in the most decent manner, are in harmony with the conclusion of the aforementioned paper.

3.4. Identifying User's Identity—Privacy Threats in Geolocation Apps/Services

Another important issue raised by a number of papers is how to address threats related to a user's identification through the disclosure of their geolocation information by malicious attackers. Duckham and Kulik [4] define privacy using Alan Westin's definition: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (p. 2), before moving to location privacy, which can be defined as "a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others" (p. 2). The authors argue that location awareness provides a specific context to users' actions. In other words, that context can endow users with a number of additional characteristics, such as social characteristics. The paper reviews a number of location privacy protection mechanisms that are not advised to be used individually; as a consequence, the authors propose a combination of approaches, such as regulation, privacy policies, anonymity, and obfuscation. Except for discussing the prerequisites under which social characteristics are expected to be shared, this paper underlines the social characteristics that provide context to the protection of location services. Users expect their location information to be handled in a way that matches their social characteristics.

In [1], Liu, Zhou, Zhu, Gao and Xiang review methods used in addressing users' location privacy concerns, such as cryptography, anonymity, obfuscation, and caching. However, the study underlines two basic obstacles in addressing location privacy, primarily due to the difficulty in making comparisons between location privacy preservation mechanisms and the incompatibility between theory and real social media practice. The authors also identify two potential types of attacks: identity and localization attack. The paper goes a step further and defines location privacy as a subcategory of information privacy by focusing on "the ability of an individual to move in public space with the expectation that under normal circumstances, their location will not be systematically and secretly recorded for later use" (p. 4). In other words, the user is willing to sacrifice part of his/her privacy while joining the public sphere as far as the user feels that the sensitive personal information will not be collected or used in a suspicious way. Another key aspect of the aforementioned study is that the representation of location information can be analyzed as a three-dimensional concept, which apart from a specific or abstract location description will also include a user's identity, spatial information (position), and temporal information (time). The study enumerates the distinctive characteristics of location information; namely, it concludes that it is massive, highly correlated, dynamic, and unequal in importance. Having stressed the importance of location information in disclosing users' identity, it is of great importance to estimate the value of privacy in terms of an actual price, as it is carried out in the following paragraph.

Danezis, Lewis, and Anderson carry out a study to focus on measuring the price of precise location information by using economic and psychology tools as a potential guide to estimate the amount that the users would be willing to pay for protecting their geolocation information [24]. Volunteers were exposed to a 'compensation auction' to determine a price that would be sufficient in order to share their exact location information, so as to make sure that participants were going to respond truthfully. The median bid according to the results was £10; however, students who were traveling outside the city or who had a partner tended to bid higher. The authors conclude that students may bid lower than the average population due to a lack of spouses, fewer responsibilities, or their environment. This study enables reaching conclusions on how individuals value their geolocation information by providing a representative amount of money for disclosing them. This representation could also be used in estimating the importance of protecting users' personal information.

Mobile devices that incorporate a variety of sensors have opened a new discussion about mobile crowd sensing (MCS). However useful these incentive mechanisms may be, they have proven to be quite costly for individual workers in terms of time and system resources. Therefore, it is important to provide the necessary incentive mechanisms to boost users' participation. Those incentives are primarily of economic origin for compensation reasons. The authors in [25] designed the INCEPTION, which is "a novel MCS system framework with an integrated design of the incentive, data aggregation, and data perturbation mechanism". In other words, it proposes a weighted data aggregation mechanism that takes into consideration users' reliability while choosing reliable workers who tend to provide reliable data so as to generate highly accurate aggregated results. The cost of the compensation for sensing and privacy leakage satisfies both truthfulness and individual rationality while minimizing the platform's total payment for worker recruiting with a guaranteed approximation ratio. Furthermore, INCEPTION guarantees maintaining users' privacy and the accuracy of the outcomes. INCEPTION was validated using both theoretical analysis and a variety of simulations.

Another paper that combines the utilization of MCS systems while protecting users' privacy is [26]. This paper sheds light upon a private incentive mechanism that protects user's privacy (worker's bid information), while at the same time aims to incentivize worker participation in MCS systems. More precisely, the author proposes a differentially private incentive mechanism that minimizes the total sum of the payment using an approximation ratio. The proposed platform collects the bids for each set of tasks, and then serves as an auctioneer in order to determine the winner while preserving the privacy of each worker against their co-workers. Except for the theoretical analysis, the paper includes an adequate number of simulations.

Yang et al. [27] also focus on designing auction-based incentive mechanisms while examining k-anonymity location privacy. As they observe the rise of location-based services (LBSs), such as Foursquare, Google Latitude, and Where, they discuss LBSs as being both informational and entertainment oriented in providing services that handle a user's geographical position. Simultaneously, they observe that users tend not to be concerned about their location privacy. Thus, the authors need to provide incentives for mobile users to participate in anonymity sets in order to achieve k-anonymity. In this paper, they examine different cases. They initiate their analysis and contribution by considering the case where all users have the same privacy degree requirement. After that, they examine the case in which they have different requirements. Last but not least, the third case refers to a more intriguing case where mobile users can disclose both valuations and requirements. The authors designed auction-based incentive mechanisms for each of the aforementioned cases while following computational efficiency, individual rationality, budget balance, and truthfulness as necessary critical properties that should be met in an auction.

This article also discusses the development of mobile services that are equipped with a variety of different sensors, thus enabling the rise of the crowdsensing paradigm according to which workers who carry mobile devices can complete several tasks related to large-scale sensory data for traffic detection (SmartRoad), transit stations labeling (TransitLabel), air quality monitoring (Aircloud), and noise map construction (Ear-phone) [28]. Location-aware and location diversity-based offline and online crowdsensing systems are put under discussion. The authors investigate offline crowdsensing, using a combinatorial algorithm to assign tasks to workers. Then, the authors introduced online crowdsensing with dynamic workers and tasks to examine changing spatio-temporal aspects. Lyapunov optimization was incorporated to handle both stochastic characteristics and a fair allocation of worker resources. In [29], Malin and Airoldi's focus is on re-identification trails and their potential privacy threats. Re-identification threats may arise through matching users' location information among different information bases. The study evaluates a number of information sets and links re-identification to the number of people to places. More specifically, using a generative model, Malin and Airoldi infer that "the skew of the distribution of people to places is one of the main factors that drives trail re-identification" (p. 413). The model under discussion estimates the risk of re-identification in case a

user's information is revealed among a set of locations. Special methods and metrics are utilized so as to investigate how different location access behaviors can trace re-identification.

The notion of "re-identification" as it was discussed in [29] is also deliberated in [30] by Bettini, Wang, and Jajodia. This paper argues that even if a user's identity is not clearly revealed, "the geo-localized history of user-requests can act as a quasi-identifier and may be used to access sensitive information about specific individuals" (p. 1). In other words, geolocation information is sensitive information, as it can potentially reveal the link between the real person and the pseudonym under use.

Managing geolocation information that may lead to defining a user's identity is tackled in [31]. More precisely, Gedik and Liu focus on how to employ a k-anonymity model in addressing location privacy concerns. The proposed model enables users to "define and modify their location privacy specifications at the granularity of single messages, including the minimum anonymity level requirement, and the inaccuracy tolerances along the temporal and spatial dimensions" (p. 17). Another important aspect of the study is the definition of the "Restricted Space Identification" and "Observation Identification" types of attack. The former addresses the possible connection among upcoming positions of the user after his identity is being revealed, and the latter refers to the matching of "external observation on location-identity binding to a message" (p. 2). The k-anonymity approach to location privacy addresses the de-personification procedure, using perturbation techniques, which are vital before distributing sensitive information to service providers. More precisely, users are given the opportunity to set their privacy preferences in relation to space and time to obscure their online traces.

According to Liu, there are two distinguishable types of location-based services: personal subscriber level privacy and corporate enterprise-level privacy [32]. This tutorial introduces location l-diversity and location m-invariant in a way that is complementary to k-anonymity so as to further support location privacy in varying location privacy demands. The former refers to the level of privacy that is linked to the user's preferences, while the latter refers to the level of privacy that is imposed by the enterprise IT experts. Some of the most popular approaches for preserving location privacy can be divided in three categories: Location protection through user-defined or system-supplied privacy policies, Location protection through the anonymous usage of information, and Location protection through applying the pseudonymity of user identities. The authors claim that "location privacy is context sensitive" (p. 2); in that way, there seems to be a continuous fluctuation between users' need for using location services appropriately and their need for protecting their privacy. In that way, by using k-anonymity, users can address their anonymity set among users, and by using l-diversity, they can address their set of possible locations. M-variant can also provide different routes for mobile users.

In [33], Jagwani and Kaushik underline that sensitive location information can potentially threaten a "user's identity and integrity" (p. 2). This type of information should be put under meticulous analysis in order to identify both possible attacks and handling mechanisms. The article draws attention to two different ways that location privacy may be affected, more precisely, the kind of information that may be derived and the amount of time that the respective information is stored. The authors list a number of possible privacy attacks along with a proposition for handling them, namely, spatial knowledge attack, location-dependent attacks, multi-query attack, maximum movement boundary attack, trajectory attacks, inversion attacks, query tracking attacks, inference attacks, and other attacks. The authors argue that despite researchers' privacy protection methods in use, especially after the Location Privacy Protection Act of 2011, there is a considerable number of open issues to address, such as the use of semantics, privacy-preserving location information collection, the application of PIR, and the formalizing of location privacy preservation mechanisms.

Additional techniques for handling a user's location information are under discussion in [34]. Freni, Ruiz Vicente, Mascetti, Bettini, and Jensen focus on location privacy, meaning information provided as far as a user's presence in a place is concerned, and absence privacy, meaning information provided as far as a user's absence from a place is concerned at a specific time. Users and service providers are highly interested in identifying and putting into practice mutually accepted privacy

preferences, as it is common knowledge that geospatial and temporal content may be retrieved through a service provider.

Another paper that deals with privacy threats associated with location privacy and friendship relation privacy while at the same time providing enough information on a user's location is [35]. According to Son, Kim, Bhuiyan, Tashakkori, Seo, and Lee, privacy is addressed as multidimensional, consisting of location privacy and identity privacy. According to Mascetti et al.'s definition of complete privacy, it is possible to refer to complete privacy when both location privacy and identity privacy are met. The authors developed a new cryptographic primitive, so that users can be protected from untrusted users while keeping their identity visible to their "friends". More precisely, the paper identifies three possible attacks, namely, attacks on pseudonym, attacks on location information, and attacks on friendship relation, which are respectively linked to pseudonym indistinguishability, identity/location privacies, and friendship relation privacy as security goals.

Duckham and Kulik also discuss the appropriate level of obfuscation for users to experience the benefits of online location services while at the same time maintaining the desired level of location privacy [8]. The authors suggest that obfuscation degrades a user's location information to protect users' privacy in pervasive computer environments as a method of balancing the amount of information required by the service in order to provide the best results and the amount of information that the user is willing to disclose. In other words, as the authors claim, "the aim of this approach is to use only just enough location information to provide a location-based service: the so-called 'need to know principle' or 'principle of minimal collection'" (p. 15). As potential negative effects can represent a considerable threat to the user, namely "location-based "spam", "personal wellbeing and safety" or "intrusive inferences" (p. 3), it is important to address through a combination of both already existing methods, such as regulation, privacy policies, anonymity, and pseudonymity and obfuscation techniques. The authors define the scenario and the architecture of the obfuscation system before proceeding to the obfuscation model and algorithms. To address potential heuristic threats, the researchers first categorize and then formalize the methodology. They conclude that the methodology needs to be implemented and tested in order to cover users' personal needs. That is to say, a user's geolocation information is thought to be descriptive and sensitive enough that researchers conclude that it is vital to be protected in the same way as a user's personal information.

As revealing geolocation information can be potentially descriptive of a user's identity, researchers have designed special applications to address this need. Mokbel, Chow, and Aref [36] present "Casper", which is "a new framework in which mobile and stationary users can entertain location-based services without revealing their location information" (p. 1). Casper includes "the location anonymizer" and "the privacy-aware query processor", as its main purpose is to deal with private information while at the same time enabling the user to take advantage of the services. Cloaked spatial information neutralizes users' sensitive location information with the use of filters.

Location-based services are also under active consideration in "Reno", which is a social location disclosure service [37]. According to Smith et al., places are described either as predefined place lists or as personally defined users' labels. Reno's pilot study was carried out to a limited number of participants and for a limited period of time, while it could only be used as a mobile phone platform for a specific mobile device. The need to protect geolocation information urged researchers to focus toward this direction while employing various means. However, while a number of different techniques and methodologies were explored, it seems that there is still the need for further research to tackle potential information leaks.

Therefore, taking into consideration the above studies and the categorization of the papers, we focused on addressing our research questions. Consequently, we proceeded in matching location information attributes to attributes of social identity in a way that could create new affiliations in addressing location privacy concerns and threats while designing privacy requirements.

3.5. Attributes of Geolocation Information and Digital Identities

According to [2], geolocation, which is a case of life-logging, can be defined as "one specific case of 'action-location': the capacity to locate the position of an object in an 'activity space' at a given time" (p. 9). Identifying user's digital identity can prove to be a multidimensional project; however, tracking a user's location information may present a detailed record of his/her activity. Location information, along with providing the setting for a user's activity (place), is also descriptive of the exact time or the part of the day in which the action was completed [22,32].

In other words, it seems that there is a connection between location information and a user's identity; thus, we proceed in examining the first research question of this paper (RQ1a: Does the interrelation of users' geospatial and social characteristics trigger additional privacy concerns and threats?), while at the same time identifying how location attributes, which have already been widely investigated [1,12,14,16,35,38], can propose new affiliations and privacy requirements in designing socially aware information systems upon the projection of location attributes on social attributes.

Drawing on Lahlou's paper, the notion of face, a basic notion of social identity theory, was introduced in our analysis as it could provide the necessary theoretical background for understanding users' different behaviors and needs in different social contexts and around the clock [2], as well as for making an analogy to the attributes of location information. According to [2], "Face is a social construct which includes both a representation of what the subject is supposed to do and of what others are supposed to do with him/her. Faces are a kind of social user's manual" (p. 18). In other words, the notion of face describes a user's identity while placing him/her in a specific context, which provides information not only for the possible way of his/her actions but also for the way other users should treat him/her for a successful interaction and cooperation among them [2].

Figure 2 shows how user's faces can function in different stages. For example, faces can be labeled as "Father", "Employee", "Patient, "Dancer", and "Tourist", etc. Social encounters are public performances that take place in specific settings, which are named "frames" by social theory. Users benefit from different faces, which can be utilized or dropped accordingly so as to warrant a successful engagement in social media practices [2].

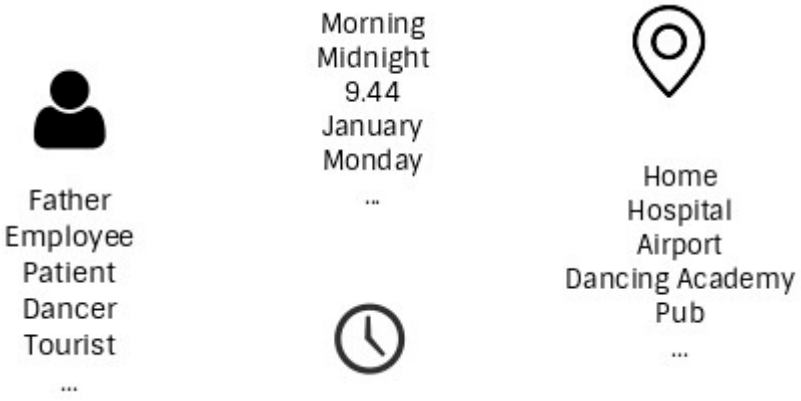

Figure 2. User's face in different stages.

Public performances are played in specific settings, which are called frames by social theory and can be paralleled to the attribute of where, according to geolocation theory. According to [10], a user's space of action can be summarized by a set of frames, i.e., by combining location information—the attribute 'where'—to time, and thus the attribute 'when'. Spaces of action are referred to as frames by social theory. As a consequence, users tend to cover different needs in alternative social settings respectively. Thus, it seems that places function as stages [4,39]. Users' social media representation (who) at a given space (when) makes them follow certain social norms (faces) [2,10].

In other words, frames (attributes of where and when) can function as stages, as they provide additional conclusions, enabling social representations to clearly require for a specific norm, expected

way of behavior, to be identified, applied, and followed from the user [2,10]. Users should be compromised to norms, as they give them the opportunity to cover their social needs in an appropriate way in order to communicate successfully through social media in their online activity space. Users reveal part of their social identities in their online social performance.

Combining frame (the attribute 'where') and time (the attribute 'when'), according to geolocation theory, we create the notion of stage, according to social theory. Stages endow social performances with additional characteristics, which enable further associations. For example, "Father" as a face can be put on in the frame "Home" during the afternoon, while "Dancer" can be utilized in the frame of "Dancing School" during the weekend.

At this point, Table 7 sheds light upon the analogy that was made among the attributes of location information and social identity. The four geolocation attributes of who, where, when, and what are linked to the attributes of social identity theory, while at the same time, there is some space for possible combinations among them.

Table 7. Attributes of Location Information and Attributes of Social Identity.

Attributes of Location Information	Attributes of Social Identity
Who	Face
Where (Space of action)	Frame
When	Time
Where (Frame) + When	Stage
What	Activity/Performance

More precisely, the attribute of 'who' in geolocation theory is analogous to the attribute of face in social theory. The attribute of 'where' can be paralleled to the frame as it refers to the space of action of the user. The attribute of 'when' is linked to the attribute of time, giving additional information about the exact or more general information about when the user proceeded in using a service or logged himself/herself during a specific action. The attribute of 'where' can be also combined to the attribute of 'when', which endows them with additional characteristics that can be paralleled to the ones of stage, according to the social theory. Last but not least, it is important to note that the attribute of 'what' can be linked to the specific activity, which is performed respectively.

3.6. Location Privacy Issues through Geolocation Information and Digital Identities Attributes

Following the analogy regarding the above attributes of location information and attributes on social identity, users' privacy concerns seem to acquire an additional aspect. In that way, this part of the results refers to the second research question of this study (RQ1b: What are the major scales measuring socio-spatial location privacy concerns?). After completing the review of the aforementioned papers, we can conclude that to the best of our knowledge, there was not a proper scale to measure users' socio-spatial location privacy concerns. Therefore, it is important to note that the focus of the study turned toward identifying the appropriate concepts that such a scale should include, connecting both social identity and geolocation information with location privacy. The interdisciplinarity of the study is discussed in the analogy between notions of social identity and location information in a way that tries to create affiliations in a reciprocal way.

By projecting location attributes on social identity attributes, we created space for addressing concerns referring to a number of additional characteristics. The notion of face draws not only to one social identity, but also to a dynamic attribute that fluctuates along with attributes of location information, such as where or when. Furthermore, it is important to note that faces are considered to be sensitive and distinctive from one another. More specifically, social actors tend not to share implications of their private life wearing one face to any other potential faces they may put on during the day [2]. For instance, users would be unwilling to share information of their "Patient" face when

wearing their "Employee" face in a distinct stage, due to potential medical information disclosure in their working environment.

In any case, combining location and time over a period of time can potentially lead to unveiling repetitive patterns, hence, enabling assumptions concerning user's habits, activity space, and the space of action-sensitive information disclosure. In that way, tracking user's online normativity through past experiences can draw inferences as far as upcoming decisions are concerned. As [2] underlines, a user's activity space places the subject in a context that is descriptive for its social status, geographic location, or future intentions. In addition, [2,9] tracking users' trajectories can potentially enable reaching conclusions about social status, geographic places, and users' ambitions, thus defining the user as a biographical subject. According to [2], activity space is "the general space of all variables that can describe a subject's state in the world: emotional state, social position, goals, geographical position, movements, belongings, etc." (p. 9). The author also defines activity as "a trajectory in this space, where behavior can be described as changes in some of these parameters" (p. 9) [2]. In other words, as location information attributes can be paralleled to users' social attributes, our analysis focuses on how these new affiliations may help designers while setting socially-aware privacy requirements. After completing our review and presenting the results of our analysis, we would like to proceed with the next section of the paper, in which we will try to increase our insight on attributes of location privacy while discussing users' socio-spatial characteristics.

4. Discussion

In a nutshell, reviewing the aforementioned studies and taking into consideration the previous analysis of our results, a number of issues regarding location privacy within social media are discussed. Deepening our understanding of geosocial networks, we have observed that geosocial services are provided in the most common social media applications that were used as case studies in different research papers, such as: Facebook, Foursquare, Twitter, and Google Latitude. At the same time, they are also available in other less popular applications, such as Grindr, Flickr, Gowalla, Loopt, and MyTown, so in that way, we can observe the dynamic presence of geosocial services dynamic in social media applications, which endorses the need for further research.

Up to this point, we have observed that geotagging services are available in social media applications, but how can users benefit in identifying themselves through representations of space? Geospatial descriptions that include social characteristics are under discussion in the definition of geosocial networks (GeoSNs), according to which geosocial networks "combine real-time location capabilities with traditional social network functionality" (p. 1) [14]. That is to say, users are willing to disclose personal information as "user-generated content". This content can include information for both a user's location, which is called "geotagging" and the presence of other users, which is called "user tagging" [14]. This definition can be linked both to Myles, Friday, and Davies argument about users option to turn their privacy into extimacy for social and entertainment purposes [7] in order to be part of the online world through representing themselves in social media applications and to the privacy paradox [40], which despite the conflict in users' minds, seems to withdraw in practice [41], as users seem to disclose private location information for both entertainment and practical reasons.

At this point, it is also interesting to discuss online relationships between users, which in most geosocial networks (GeoSNs) can be symmetric; in others words, two users should mutually accept each other before sharing information [14]. An example of that can be the "Friend" notion as it is used in Facebook. On the other hand, another type of relationship between users can be the asymmetric one, meaning that users can follow other users without being mutually accepted; approval is not required before being able to obtain access to a user's personal information. An example of that type of relationship could be the notion of followers on Twitter. This observation creates space for revising the question of who has access to our information, for what reason, and under which circumstances [21,22]. According to [1], the authors identify three attributes of location privacy: namely, identity, position, and time—in other words, information related to who, where, and when, respectively.

Regarding the attribute 'who', the user can be identified as far as his/her name, gender, or member of a community/population/geographic position are concerned. The attribute 'where' signifies information referring to the user's exact x and y: the neighborhood, city, island, or municipality. The attribute 'when' reveals information concerning exact time in hours and minutes, a part of the day description, and reference to the day, week, month, and year.

In our analysis, activity was also included as an attribute to identify the fourth attribute of location information: the attribute 'what', which is linked to the user's activity, i.e., his/her occupation, recreation time, sleeping, eating, walking, etc. activities [1]. In addition, Lefebvre's analysis of the social body also points toward the same direction as it further supports both the interrelation between social and location attributes through the four aforementioned common attributes of our analysis, and at the same time provides evidence regarding the need for being in compliance with location privacy when designing privacy-aware information systems [18].

In this regard, it is important to focus on the analogy that was made among the attributes of location information and social identity, while presenting it in a systematic way so as to identify the location privacy information that should be taken into consideration in order to address location privacy issues. Table 8 summarizes the identified four attributes of location privacy that combine socio-spatial characteristics.

Table 8. Attributes of Location Privacy Related to Users' Socio-Spatial Characteristics.

Attributes of Location Privacy Related to Users' Socio-Spatial Characteristics		
Who (user's identity information)	Name, Gender, Nationality, Membership	Indication of his/her actual name (John), gender (M/F), a photograph of him/herself or membership in a specific group (English teacher, Erasmus participant, Salsa in the city)
Where (spatial information)	Neighborhood, City, Municipality	Disclosure of exact spatial information (x,y), use of a landmark (Statue of Liberty, Mytilene), use of hashtags (#Mytilene), or use of a photograph of the place
When (temporal information)	Hours, Minutes, Day, Week, Month	Disclosure of exact temporal information (hh:mm:ss), use of hashtags (#good morning), or use of a photograph with light depiction
What (occupational information)	Activity, Occupation	Disclosure of exact activity (studying), use of hashtag (#dancing), unveiling of occupation (yoga instructor, 3D printer specialist, playing the guitar) or use of a photograph doing an activity

Each attribute (who, where, when, what) can be described in a scale, starting from a rather vague description, moving to more detailed information or even providing the utmost level of granularity (state the exact name, location, time, and activity of the user). Vague information about location attributes can be linked to location privacy techniques addressing users' privacy concerns, while more detailed information or a combination of the aforementioned attributes enables reaching conclusions or potentially targeting the user.

Users' habits can be also identified through combining location attributes. For instance, even if the attribute 'who'—in other words, the face of a user, which is also indicative of his/her digital identity at a specific frame and time (stage)—is protected through obfuscation, and thus not identifiable from malicious users, the combination of the attribute 'who' to the attribute 'where' (space of action, frame), 'when' (time), or 'what' (activity, performance) can be descriptive enough in order to reveal sensitive information about the user [42]. Combining all four location attributes can enable quite precise predictions about user's online normativity. Figure 3 attempts a visual representation in order

to illustrate how social and location attributes may reflect users' representation of their digital identity in social media.

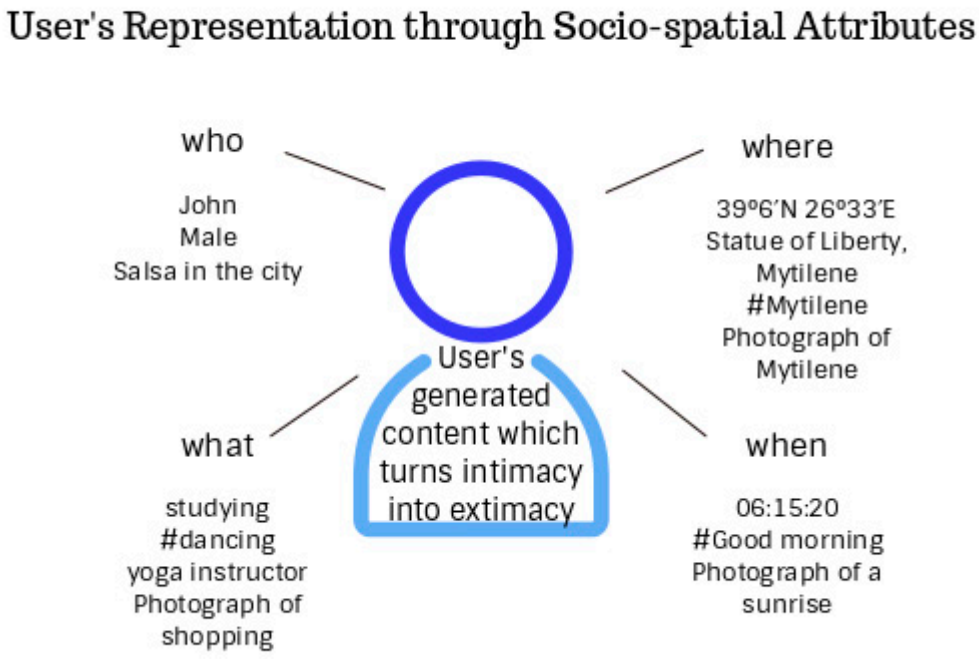

Figure 3. User's representation through socio-spatial attributes.

Social actors are affected by previous experiences while making future choices [2], so tracking users' trajectory using location information facilitates assumptions about user's normativity, as future choices can be inferred through past records on social status, geographic places, and users' ambitions, which will have already defined users as biographical subjects [2,10]. Users' online behavior that is illustrated in a specific place and time respectively will constitute an online habit, which will be descriptive enough to create affiliations and correlations for identifying not only a user's identity but also their future options and the relationships among them. That is why location–privacy protection mechanisms (LPPMs) use a number of techniques to protect this sensitive information [21,43], while at the same time users tend to express their concerns on potential threats. Combining attributes of social identity to location attributes may disclose information concerning users' privacy in a way that arises additional privacy issues. Thus, taking these new affiliations into consideration while summarizing the reviewed papers for our analysis, the need for users to protect their privacy became evident. This need was important to provide the necessary questions to design our methodology before trying to address those privacy issues.

5. Conclusions

The main contribution of this paper is to broaden understanding of the way that users' social characteristics intertwined with users' geolocation information can create new affiliations for addressing location privacy issues. Focusing on geosocial networks, a user's identity through geolocation information, and location privacy concerns and threats, we provide a set of targeted location privacy attributes in combination with user's socio-spatial characteristics, underlining the necessity for the development of a methodology that should propose appropriate scales in measuring a user's location privacy threats, enabling researchers to open up innovative approaches.

Despite our contribution, it is also important to note the limitations of the paper. Our study focuses on social characteristics through the notion of face in an effort to examine social characteristics from a more socially oriented point of view. Although in our initial design, it seems that face is still a quite general and complex notion that needs further analysis in order for researchers to draw

conclusions regarding specific users' faces both around the clock and in different settings to proceed in addressing location privacy concerns.

Future research on this topic [1–3,44] will greatly contribute to designing and proposing a socially and geologically aware methodology for addressing users' concerns. Future research will also intentionally specify and formulate appropriate measurement scales for identifying users' privacy, addressing both social and geospatial characteristics by paying attention to attributes of location information and digital identity, which are perceived as a subcategory of social identity in the current study. Another point worth mentioning for future work could also be examining whether all a user's concerns have already been covered bibliographically, of if there are any additional concerns or threats that should be covered by upcoming research questions.

Author Contributions: K.V. contributed to the investigation of social and location attributes and the writing of the original draft. A.K. contributed to the analysis and visualization of the work as well as the research regarding the social aspects and their correlation with privacy. C.K. contributed to the conceptualization of the idea as well as the supervision and writing, review, and editing. D.K. contributed to the investigation of the geolocation aspects, and S.G. contributed to the supervision and writing, review, and editing of the paper.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Liu, B.; Zhou, W.; Zhu, T.; Gao, L.; Xiang, Y. Location Privacy and Its Applications: A Systematic Study. *IEEE Access* **2018**, *6*, 17606–17624. [CrossRef]
2. Lahlou, S. Identity, social status, privacy and face-keeping in digital society. *Soc. Sci. Inf.* **2008**, *47*, 299–330. [CrossRef]
3. Lenberg, P.; Feldt, R.; Wallgren, L.G. Behavioral software engineering: A definition and systematic literature review. *J. Syst. Softw.* **2015**, *107*, 15–37. [CrossRef]
4. Duckham, M.; Kulik, L. Location privacy and location-aware computing. In *Dynamic & Mobile GIS: Investigating Change in Space and Time*; CRC Press: Boca Raton, FL, USA, 2006; Volume 3, pp. 35–51.
5. Acquisti, A.; Gross, R. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In Proceedings of the Privacy Enhancing Technologies, PET 2006, Cambridge, UK, 28–30 June 2006; Danezis, G., Golle, P., Eds.; Springer: Berlin/Heidelberg, Germany, 2006; pp. 36–58.
6. Herrmann, M.; Hildebrandt, M.; Tielemans, L.; Diaz, C. Privacy in Location-Based Services: An Interdisciplinary Approach. *SCRIPTed* **2016**, *13*, 144. [CrossRef]
7. Myles, G.; Friday, A.; Davies, N. Preserving privacy in environments with location-based applications. *IEEE Pervasive Comput.* **2003**, *2*, 56–64. [CrossRef]
8. Duckham, M.; Kulik, L. A Formal Model of Obfuscation and Negotiation for Location Privacy. In *Pervasive Computing*; Gellersen, H.-W., Want, R., Schmidt, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3468, pp. 152–170, ISBN 978-3-540-26008-0.
9. Miguel, C.; Medina, P. The Transformation of Identity and Privacy through Online Social Networks (The CouchSurfing Case). 2011. Available online: http://eprints.leedsbeckett.ac.uk/2159/1/The%20Transformation%20of%20Identity%20and%20Privacy_The%20CouchSurfing%20Case.pdf (accessed on 9 January 2019).
10. Jenkins, R. *Social Identity*, 3rd ed.; Key Ideas; Routledge: London, UK; New York, NY, USA, 2008; ISBN 978-0-415-44848-2.
11. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *PLoS Med.* **2009**, *6*, e1000097. [CrossRef] [PubMed]
12. Birnholtz, J.; Fitzpatrick, C.; Handel, M.; Brubaker, J.R. Identity, identification and identifiability: The language of self-presentation on a location-based mobile dating app. In Proceedings of the 16th International Conference on Human-Computer Interaction with Mobile Devices & Services, Toronto, ON, Canada, 23–26 September 2014; pp. 3–12.
13. Puttaswamy, K.P.N.; Wang, S.; Steinbauer, T.; Agrawal, D.; Abbadi, A.E.; Kruegel, C.; Zhao, B.Y. Preserving Location Privacy in Geosocial Applications. *IEEE Trans. Mob. Comput.* **2014**, *13*, 159–173. [CrossRef]

14. Ruiz Vicente, C.; Freni, D.; Bettini, C.; Jensen, C.S. Location-Related Privacy in Geo-Social Networks. *IEEE Internet Comput.* **2011**, *15*, 20–27. [CrossRef]
15. Tang, K.P.; Lin, J.; Hong, J.I.; Siewiorek, D.P.; Sadeh, N. Rethinking location sharing: Exploring the implications of social-driven vs. purpose-driven location sharing. In Proceedings of the 12th ACM International Conference on Ubiquitous Computing, Copenhagen, Denmark, 26–29 September 2010; pp. 85–94.
16. Bao, J.; Zheng, Y.; Mokbel, M.F. Location-based and preference-aware recommendation using sparse geo-social networking data. In Proceedings of the 20th International Conference on Advances in Geographic Information Systems—SIGSPATIAL '12, Redondo Beach, CA, USA, 7–9 November; ACM Press: Redondo Beach, CA, USA, 2012; p. 199.
17. Schwartz, R.; Halegoua, G.R. The spatial self: Location-based identity performance on social media. *New Media Soc.* **2015**, *17*, 1643–1660. [CrossRef]
18. Simonsen, K. Bodies, sensations, space and time: The contribution from henri lefebvre. *Geogr. Ann. Ser. B Hum. Geogr.* **2005**, *87*, 1–14. [CrossRef]
19. Scellato, S.; Musolesi, M.; Mascolo, C.; Latora, V. Distance Matters: Geo-social Metrics for Online Social Networks. In Proceedings of the 3rd Conference on Online Social Networks, USENIX Association, Boston, MA, USA, 22–22 June 2010; Volume 9, p. 8.
20. Mascetti, S.; Freni, D.; Bettini, C.; Wang, X.S.; Jajodia, S. Privacy in geo-social networks: Proximity notification with untrusted service providers and curious buddies. *VLDB J.* **2011**, *20*, 541–566. [CrossRef]
21. Snekkenes, E. Concepts for Personal Location Privacy Policies. In Proceedings of the 3rd ACM Conference on Electronic Commerce, Tampa, FL, USA, 14–17 October 2001; ACM: New York, NY, USA, 2001; pp. 48–57.
22. Consolvo, S.; Smith, I.E.; Matthews, T.; LaMarca, A.; Tabert, J.; Powledge, P. Location disclosure to social relations: Why, when, & what people want to share. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Portland, OR, USA, 2–7 April 2005; pp. 81–90.
23. Grice, H.P. Logic and Conversation. 1975. Available online: http://www.communicationcache.com/uploads/1/0/8/8/10887248/logic_and_conversation.pdf (accessed on 9 January 2019).
24. Danezis, G.; Lewis, S.; Anderson, R.J. How much is location privacy worth? In Proceedings of the 4th Annual Workshop on the Economics of Information Security (WEIS 2005), Cambridge, MA, USA, 1–3 June 2005; Volume 5.
25. Jin, H.; Su, L.; Xiao, H.; Nahrstedt, K. Incentive Mechanism for Privacy-Aware Data Aggregation in Mobile Crowd Sensing Systems. *IEEE/ACM Trans. Netw.* **2018**, *26*, 2019–2032. [CrossRef]
26. Jin, H.; Su, L.; Ding, B.; Nahrstedt, K.; Borisov, N. Enabling Privacy-Preserving Incentives for Mobile Crowd Sensing Systems. In Proceedings of the 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS), Nara, Japan, 27–30 June 2016; pp. 344–353.
27. Yang, D.; Fang, X.; Xue, G. Truthful incentive mechanisms for k-anonymity location privacy. In Proceedings of the 2013 Proceedings IEEE INFOCOM, Turin, Italy, 14–19 April 2013; pp. 2994–3002.
28. Wang, X.; Jia, R.; Tian, X.; Gan, X. Dynamic Task Assignment in Crowdsensing with Location Awareness and Location Diversity. In Proceedings of the IEEE INFOCOM 2018—IEEE Conference on Computer Communications, Honolulu, HI, USA, 15–19 April 2018; pp. 2420–2428.
29. Malin, B.; Airoldi, E. The Effects of Location Access Behavior on Re-Identification Risk in a Distributed Environment. In Proceedings of the Privacy Enhancing Technologies, Cambridge, UK, 28–30 June 2006; Danezis, G., Golle, P., Eds.; Springer: Berlin/Heidelberg, Germany, 2006; pp. 413–429.
30. Bettini, C.; Wang, X.S.; Jajodia, S. Protecting privacy against location-based personal identification. In Proceedings of the Workshop on Secure Data Management, Trondheim, Norway, 2–3 September 2005; pp. 185–199.
31. Gedik, B.; Liu, L. Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms. *IEEE Trans. Mob. Comput.* **2008**, *7*, 1–18. [CrossRef]
32. Liu, L. From data privacy to location privacy: Models and algorithms. In Proceedings of the 33rd International Conference on Very Large Data Bases, Vienna, Austria, 23–27 September 2007; pp. 1429–1430.
33. Jagwani, P.; Kaushik, S. Privacy in Location Based Services: Protection Strategies, Attack Models and Open Challenges. In *Information Science and Applications 2017*; Kim, K., Joukov, N., Eds.; Springer Singapore: Singapore, 2017; Volume 424, pp. 12–21, ISBN 978-981-10-4153-2.

34. Freni, D.; Ruiz Vicente, C.; Mascetti, S.; Bettini, C.; Jensen, C.S. Preserving location and absence privacy in geo-social networks. In Proceedings of the 19th ACM International Conference on Information and Knowledge Management—CIKM '10, Toronto, ON, Canada, 26–30 October 2010; ACM Press: Toronto, ON, Canada, 2010; p. 309.
35. Son, J.; Kim, D.; Bhuiyan, M.Z.A.; Tashakkori, R.; Seo, J.; Lee, D.H. Privacy Enhanced Location Sharing for Mobile Online Social Networks. *IEEE Trans. Sustain. Comput.* **2018**. [CrossRef]
36. Mokbel, M.F.; Chow, C.-Y.; Aref, W.G. The new casper: Query processing for location services without compromising privacy. In Proceedings of the 32nd International Conference on Very Large Data Bases, Vienna, Austria, 23–27 September 2006; pp. 763–774.
37. Smith, I.; Consolvo, S.; Lamarca, A.; Hightower, J.; Scott, J.; Sohn, T.; Hughes, J.; Iachello, G.; Abowd, G. Social disclosure of place: From location technology to communication practices. *Pervasive Comput.* **2005**, *3468*, 151–164.
38. Cramer, H.; Rost, M.; Holmquist, L.E. Performing a check-in: Emerging practices, norms and 'conflicts' in location-sharing using foursquare. In Proceedings of the 13th international conference on human computer interaction with mobile devices and services, Stockholm, Sweden, 30 August–2 September 2011; pp. 57–66.
39. Barkhuus, L.; Dey, A.K. Location-Based Services for Mobile Telephony: A Study of Users' Privacy Concerns. In *Human-Computer Interaction—INTERACT 2009*; Interact: Zurich, Switzerland, 2003; Volume 3, pp. 702–712.
40. Is Opposition to GM food Irrational? 2015. Available online: https://www.bbc.com/news/science-environment-32901834 (accessed on 9 January 2019).
41. Kokolakis, S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Comput. Secur.* **2017**, *64*, 122–134. [CrossRef]
42. Vgena, K.; Kitsiou, A.; Kalloniatis, C.; Kavroudakis, D. Do Identity and Location Data Interrelate? New Affiliations and Privacy Concerns in Social-Driven Sharing. In *Trust, Privacy and Security in Digital Business*; Gritzalis, S., Weippl, E.R., Katsikas, S.K., Anderst-Kotsis, G., Tjoa, A.M., Khalil, I., Eds.; Springer International Publishing: Cham, Switzerland, 2019; Volume 11711, pp. 3–16, ISBN 978-3-030-27812-0.
43. Beresford, A.R.; Stajano, F. Location privacy in pervasive computing. *IEEE Pervasive Comput.* **2003**, *2*, 46–55. [CrossRef]
44. Storey, M.-A.; Treude, C.; van Deursen, A.; Cheng, L.-T. The impact of social media on software engineering practices and tools. In Proceedings of the FSE/SDP Workshop on Future of Software Engineering Research, Santa Fe, NM, USA, 7–11 November 2010; pp. 359–364.