Location privacy and public metadata in social media platforms: attitudes, behaviors and opinions

Multimedia Tools And Applications manuscript No.
(will be inserted by the editor)

Location privacy and public metadata in social media platforms: attitudes, behaviors and opinions

Marco Furini, Valentina Tamanini

Dipartimento di Comunicazione ed Economia
Università di Modena e Reggio Emilia
Reggio Emilia, Italy.
E-mail: marco.furini@unimore.it
Ph. +39-0522-523156
Fax. +39-0522-523055

The date of receipt and acceptance will be inserted by the editor

Abstract The high availability of geolocation technologies is changing the social media mobile scenario and is exposing users to privacy risks. Different studies have focused on location privacy in the mobile scenario, but the results are conflicting: some say that users are concerned about location privacy, others say they are not. In this paper, we initially investigate attitudes and behaviors of people toward a location-aware scenario; then, we show users the amount of personal and sensitive data that can be extracted from contents publicly available in social platforms, and finally we ask for their opinions about a location-aware scenario. Results show that people who were not initially concerned about privacy are the most worried about the location-aware scenario; conversely, people who were initially concerned are less worried about the location-aware scenario and find the scenario interesting. A deeper analysis of the obtained results allows us to draw guidelines that might be helpful to build an effective location-aware scenario.

1 Introduction

Knowledge of user location plays an important role in society and is likely to be of critical importance in future social-based applications. Many advanced information systems may use geolocation technologies to identify user location in order to provide customized services by delivering localized news, recommending friends, serving targeted ads, improving large scale systems (e.g., cloud computing, content-based delivery networks). The possibilities

are so broad that location-aware social applications are likely to be important for the next generation mobile computing [1]. Indeed, novel location-aware social applications may be employed in many different scenarios like urban planning, human mobility, health monitoring, security, advertising, emergency and altruistic services [2–10]. For instance, after an incident, law enforcement agencies may spend many person-months to find images shot near a specific address in order to find a suspect or other evidence [9]. The knowledge of who were in the area or the automatic gathering of pictures taken by people in the area would be of great help. Similarly, in a crisis scene, such as a street accident or a terrorist attack, rescue teams may take hours to reach the area and organize the necessary operations and therefore it would be useful to provide first responders with real-time pictures/videos of the emergency while still driving toward the crisis area [2]. In this case, the knowledge of who is in the area may give access to real-time hazards, disaster information, photos and video that would likely speed-up the rescue operations.

In this social media mobile scenario, user's geographical location can be generated either by users (through voluntary check-in in applications like Foursquare and Facebook Places) or by applications (through technologies like IP address geolocation, cellphone network triangulation, RFID and GPS). Regardless of the used approach, the result is that the produced content is coupled with the geographical location where the user produced it. Moreover, in addition to geolocation information, many applications attach to users' contents a lot of other information like OS language, device type and capture time. As a result, by tweeting, posting or taking pictures, users produce and share a vast amount of personal information.

Users consider the social media mobile scenario exciting, but it is worth mentioning that most of the information attached to the contents (i.e., metadata) can be considered personal and sensitive. Indeed, third parties may combine location data with other information to trace, in real-time, the movement of a single user. Similarly, criminals may be facilitated in their activities (from burglary and theft, to stalking, kidnapping and domestic violence) as geolocation data may reveal personal information such as home, work and school address [11]. Therefore, users should be aware of possible privacy and security risks when using location-aware social applications [12].

In the literature, there has been a significant amount of research on location privacy, but results are not always clear and consistent. For instance, if on the one side Kelly et al. [13] showed that users' strong privacy concerns may hinder the adoption of systems leveraging this potentially to third parties, on the other side Chin et al. [14] showed that most people are willing to share their location when using mobile applications. Conflicting results are likely due to the infancy stage of the location-aware scenario but, in our opinion, another important reason is the small number of users in the analyzed sample (e.g., 16 participants in [12], 27 participants in [13], 60 participants in [14], 18 participants in [15]), which may affect the obtained results.

Our hypothesis is that, due to the infancy stage of the location-aware scenario, people ignore many of its features and this lack of knowledge may influence the location-privacy investigation. For this reason, in this paper, we use a different approach to understand attitudes, behaviors and opinions of users toward the novel location-aware scenario. We split the investigation into two phases: the first phase aims at understanding what people know or ignore of a location-aware scenario; the second phase investigates users' opinions after showing them a simple location-aware application able to extract personal and sensitive data from users' contents publicly available in social media platforms and able to use these data to locate, in real-time, these users on a map and to show the obtained personal and sensitive information. By splitting the investigation into two phases, the analysis will highlight not only attitudes, behaviors and opinions of users, but will also reveal if there is a relation between what people know about the location-aware scenario and what people really think about privacy.

Results obtained from the first phase show that people are not concerned about privacy, but, in the second phase, these people are the most worried about the location-aware scenario; conversely, people who were initially concerned, are less worried about the location-aware scenario and find the scenario interesting. Results also show that men are more willing than women to enter the location-aware scenario, but both require to give authorization and to receive benefits when third parties access to their contents. Other interesting findings are that users do not want to be bothered with marketing or advertising services, that photos are considered private resources to be protected from third parties access, and that women are very alarmed if third parties would access to their photos.

The obtained results are used to outline possible guidelines for both users and developers/enterprises that we think might be helpful to develop an effective location-aware scenario.

The remainder of this paper is organized as follows: Section 2 presents related works in the area of location-aware applications; Section 3 investigates users' attitudes and behaviors toward location privacy; Section 4 shows details of the application developed to create a location-aware scenario and Section 5 investigates opinions and preferences with respect to this scenario. In Section 6 we propose some guidelines for the development of an effective location-aware scenario. Conclusions are drawn in Section 7.

2 Related Work

In the mobile scenario, geolocation technologies are increasingly exploited by novel services and applications. Many different location-aware applications are available for download in the various app-stores and users are excited about customized services. For instance, Foursquare and Facebook Places, two well-known location-aware applications, combine the social aspect with geolocation data in order to encourage users to "check-in" their current

position from a list of venues the application locates nearby to let friends know where they are. As a result, by using these applications, one can easily see if any of his/her friends have checked-in in the nearby.

In addition to applications available in the various app-stores, other examples of location-aware applications include the ones developed by researchers to study specific topics. For instance, Cho et al. [5] studied the relation among human geographic movement, its temporal dynamics, and the ties of the social network. In particular, they analyzed the role of geography and daily routine on human mobility patterns and the effect of social ties. The motivation of the study was to seek and identify the fundamental factors that govern human mobility. Bicocchi et al. [16] developed a mobile application that continuously collects and stores user's location in order to automatically write a whereabouts diary.

Within the location-aware scenario, applications where users voluntarily check-in are only a portion. Indeed, many other applications collect geolocation information without asking users to check-in to specific places. These data are critical and fundamental for some applications (e.g., maps services), but are not necessary to some others (e.g., music services). For instance, in Twitter, geolocation information are not critical for the service, nor they are critical for the service offered by Instagram or Shazam[1]. Why users should grant these applications the access to their personal geolocation data? Do users know that they are sharing personal sensitive data while using geolocation technologies?

Different studies focused on the privacy issue related to disclosing personal geolocation to third-party applications and results do not completely clarify the scenario. Jedrzejczyk et al. [17] highlighted that users are not very good at privacy settings and they usually accept the default options; things are a little bit different if they understand the future implications of their choices. Therefore, they propose to use ad-hoc warnings on the user's mobile display to aware users. A subsequent study by Fisher et al. [18] highlighted that users reflexively click "OK" on warning messages and that some applications are more trusted than others. In particular, with respect to geolocation data, users are willing to disclose personal data when these information are critical for the application: 97% of the interviewed disclosed their geolocation data to geomap applications, while the percentage dropped to 53% when music applications asked for location data.

Kelly et al. [13] presented an empirical investigation of people attitudes towards sharing of personal geolocation with mobile advertisers. In particular, they showed that users' strong privacy concerns might hinder the adoption of systems leveraging this potentially invasive form of advertising. However, their study also found that advanced privacy settings may help alleviating some of these concerns and their findings suggest that if future systems will have usable privacy settings, then all entities involved will receive benefits from the sharing of personal information.

[1] A music identification service available through a mobile app.

Chin et al. [14] highlighted that the type of applications plays a critical role in users' experiences with their smartphones and they found that users are more concerned about privacy when using smartphones than laptops. Through structured interviews, the study showed how users are reluctant to enter very sensitive personal information like social security number or bank account information, but feel free to share personal information like photos and geolocation data.

Madden et al [19] focused on privacy and teens in the social media scenario. Their results show that teens are sharing more personal information on their profiles than in the past and most of them are not very concerned about third parties accessing to their data. With respect to the sharing of personal location, 16% of teen social media users have set up their profile to automatically include their location in posts.

The above studies highlighted that the location-aware scenario is subject to different findings. In this paper, we aim at clarifying some aspects of this novel scenario. For instance, do users know that some of the applications they use collect geolocation data? What do users think about location-aware services? Do users change their opinion when they find out that third parties may access to users' personal and sensitive data by simply accessing to contents publicly available in social media platforms?

3 Users' attitudes toward privacy in location-based applications

In order to build an effective location-aware scenario, it is necessary to understand users' attitudes toward privacy. Unfortunately, as shown in the previous section, some studies say users are concerned about privacy, while other studies say they are not. In our opinion, these conflicting results are mainly due to: i) the infancy stage of the location-aware scenario, and ii) the small number of users in the sample (e.g., 16 participants in [12], 27 participants in [13], 60 participants in [14], 18 participants in [15]). Needless to say, this lack of clarity may represent a burden for the success of location-based applications.

Through a real-world study, we aim at understanding what people think about novel services and applications based on geolocation technologies. In particular, we are interested in attitudes and behaviors of people who daily use technological devices and mobile applications, who consider mobile devices and applications as commodities and not as technological pieces of hardware to be scared of. Indeed, these people are usually considered early adopters of new technologies and services, and therefore, by focusing on them and by investigating their current attitudes and behaviors, we likely have insights of what will happen in the future location-aware scenario. To get in touch with these people, we asked for voluntary participants through different technological platforms (social networks, emails and forums) and we did not specify any age limit.

We have been contacted by 122 people (2 to 6 times the number of participants to other studies in the field) and Figure 1 reports the charac-

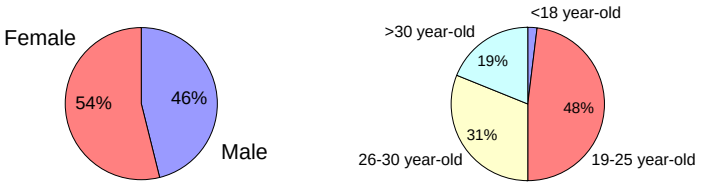

Fig. 1 Characteristics of the subjects who voluntarily participated to our real-world study: sex (left) and age (right).

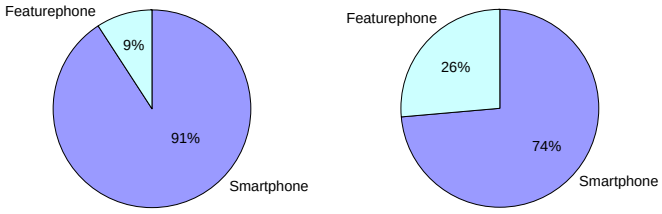

Fig. 2 Smarthphone penetration: men (left) and women (right).

teristics of the 122 participants: 54% are women and 46% are men. Two percent of the respondents are younger than 18 year-old, 48% are between 19 and 25, 31% are between 26 and 30 and 19% are older than 30 year-old. Results show a first interesting finding: the majority of people who daily use technological devices and mobile applications are 19-30 years old.

In the following, we present results obtained while investigating technological equipment and individual habits, and the relationship between users and location-aware applications like Twitter and Instagram.

3.1 Technological equipment and habits

One of the goals of the questionnaire was to understand the technological equipment (smartphone penetration, availability of GPS technology) and the users' habits in the mobile scenario (data subscription plan, download of mobile applications and usage of geolocation services).

Figure 2 (left) reports the type of cellphone owned by respondents: smartphone or featurephone. Results show that smartphone penetration is very high: 91% among men and 74% among women. We investigated whether these smart devices are connected to the Internet or not: 92% of respondents said their device is always connected through flat rate data plans. Therefore, access to the Internet through smartphone devices is very common among respondents.

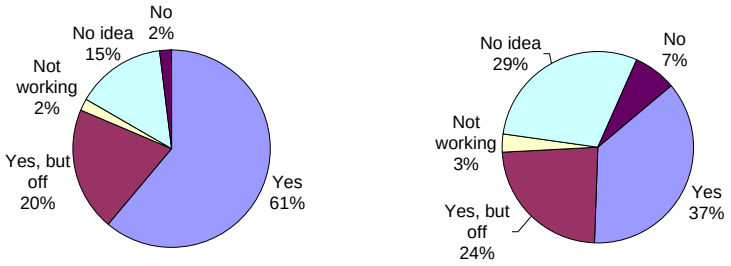

Fig. 3 GPS availiability within smarthphone owners: men (left) and women (right).

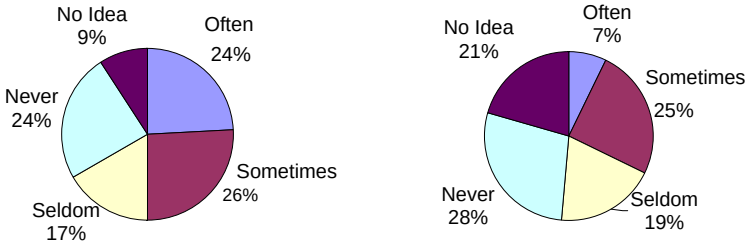

Fig. 4 Use of location-aware mobile applications: men (left) and women (right).

Figure 3 reports the presence of GPS technology in smartphone devices owned by participants: 83% of men and 64% of women claim to have GPS technology over their smartphones. Looking at the people who keep the GPS active, we can observe a different behavior between men and women: 61% of men keep the GPS on, but the percentage decreases to 37% when analyzing women. Another interesting difference is that 15% of men and 29% of women have no idea about GPS availability.

Figure 4 reports the use of location-aware mobile applications among respondents. Men seem to be more familiar with these applications (67% vs. 51%), but it is worth noting that the percentage of people who have no idea about location-aware applications is higher among women (21%) than among men (9%).

To better understand the behavior of the respondents with respect to the use of location-aware applications, Figure 5 shows the behavior of people who keep the GPS on and the behavior of those who have no idea about GPS availability over their devices. When considering the behavior of people who keep the GPS on, we expected to have a rate close to 100%, but instead only 77% of respondents claim to use location-aware applications, meaning that one in five (21%) keep the GPS on, but do not use location-aware applications. When considering people who have no idea about GPS availability

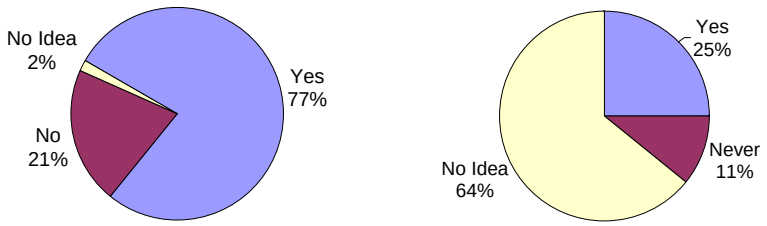

Fig. 5 Use of location-aware mobile applications by considering respondents with GPS on (left) and respondents with "No idea" about GPS availability (right).

within their smartphones (Figure 5-right), 25% claim to use location-aware applications and 64% continue to have no idea.

Although the location-aware scenario is its infancy stage, results show that location-aware applications are quite popular. However, results also show that people have a poor grasp of technologies/applications they use.

3.2 Twitter and Instagram Presence

The second main goal of the questionnaire was to understand how users share their contents in social platforms. It is worth noting that we focused on Twitter and on Instagram because, after an experimental investigation, we observed that these platforms present a large volume of publicly accessible data (no need to log-in, no need to be friend to see someone's tweets/photos) and provide valuable information to locate users.

Figure 6 reports data obtained by asking participants whether they have a Twitter account. Men are more familiar with the micro-blogging platform than women (72% vs. 57%) and among those who have a Twitter account, 48% of men and 32% of women actually use it, whereas 24% of men and 25% of women just registered to the platform but claim not to use it.

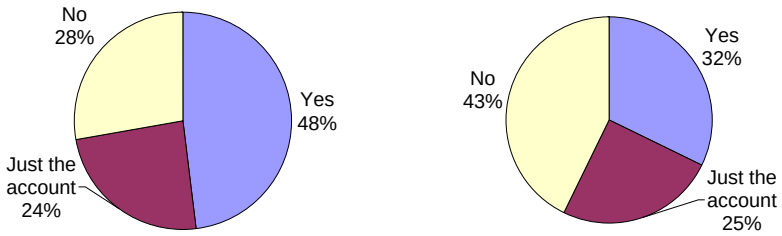

Fig. 6 Twitter presence: men (left) and women (right).

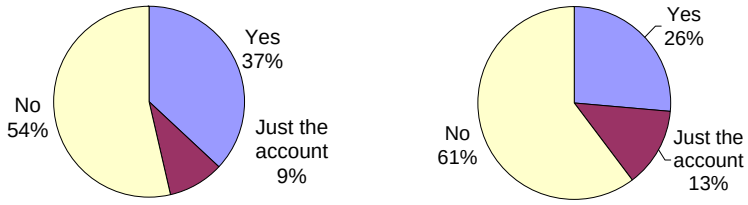

Fig. 7 Instagram presence: men (left) and women (right).

Figure 7 presents the same investigation, but in the Instagram scenario. It is to note that the majority of the respondents do not have an Instagram account (54% of men and 61% of women). Probably, the reason is that Instagram is a recent application and therefore it is not as popular as Twitter. However, results show that men are more familiar with the mobile photo-sharing platform than women (46% vs. 39%) and among those who have an account, 37% of men and 26% of women actually use it.

Since both Twitter and Instagram may access to the location-aware technology available in the smartphone and may attach location information to the produced contents, we investigated the penetration of these applications among people who claim to use location-aware applications. Figure 8 shows that both applications are popular among people who use location-aware applications: 73% of them have a Twitter account and 59% of them have a Instagram account. In particular, almost half of them regularly use Twitter (48%) or Instagram (45%).

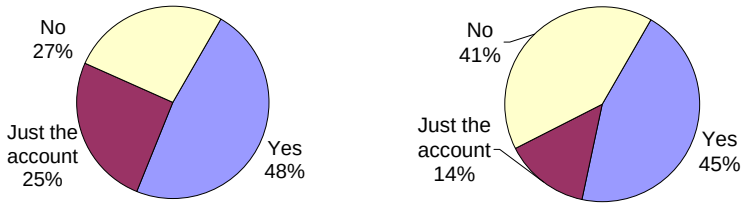

Fig. 8 Twitter (left) and Instagram (right) presence by considering people who use location-aware applications.

The presence in Twitter/Instagram can be different from person to person since the platforms provide two different profiles: private or public. In both platforms, the default setting is public (tweets/photos are visible to anyone, whether or not they have an account) and, therefore, to protect

tweets/photos (visible only to approved friends) users have to change the profile setting. To understand the way users share their contents, we investigated the type of profile they have on the two platforms.

Figure 9 reports results obtained while asking participants the profile they use on Twitter. A considerable number of respondents (37% of men and 51% of women) ignore the characteristics of their profile. The private profile is selected by a minority of people: 28% of men and 24% of women.

Similar results can be observed in Figure 10, where we report results obtained while asking participants the profile they have on the Instagram platform: 59% of men and 68% of women have no idea about the nature of their profile. Only 41% of men know their profile (13% of them opted for a private profile); the percentage decreases to 32% when looking at the women behavior (10% of them opted for a private profile).

The high percentage of people who have no idea about the nature of their profile implies that they ignore who can access to their generated contents. By considering that a considerable percentage of people opted for a public profile, it is reasonable to assume that the majority of generated contents are publicly available on the two platforms. Since Twitter and Instagram may attach user's geographical location to the generated contents, it is likely that these contents may contain personal and sensitive data. To better understand this aspect, we ask participants if they use the geolocation feature available in Twitter and in Instagram.

Figure 11 reports the use of the geolocation feature within Twitter. If the percentage of people who do not use this feature is similar among men and women (30% vs. 37%), there is a different behavior when analyzing people who use this feature: 31% of men vs. 10% of women. Also, it is worth noting the percentage of people who ignore the usage of this feature (39% of men and 53% of women).

Figure 12 shows the use of the geolocation feature within Instagram. With respect to Twitter, men are less familiar with this feature (59% of them have no idea against the 39% of the Twitter users), but among the ones who do have idea about the feature, 35% of them claim to use the feature, and only 6% of them claim not to. A similar difference can be noted

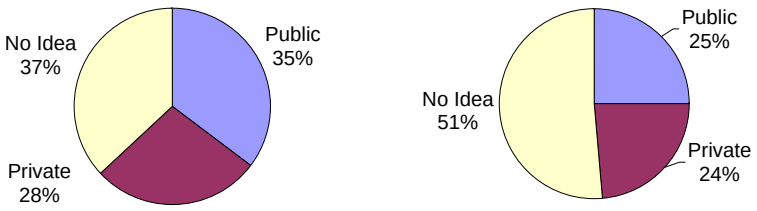

Fig. 9 Twitter profile used by respondents: men (left) and women (right).

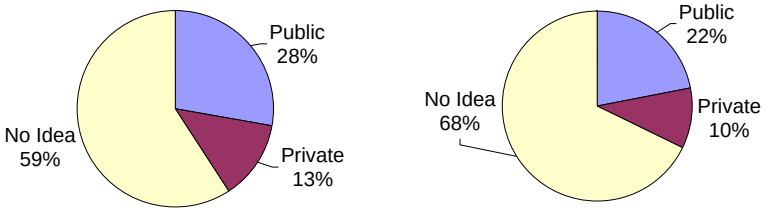

Fig. 10 Instagram profile used by respondents: men (left) and women (right).

when observing the women behavior: 66% (against the 53% of Twitter) have no idea about the use of this feature, and 18% (against 10% measured in the Twitter investigation) of them claim to use the geolocation feature.

Results highlight that the majority of respondents have no idea about the available features and also highlight that only a minority of the respondents claim not to use the geolocation feature. Furthermore, the obtained results show that people tend to use this feature more when sharing photos than when sharing tweets. By combining these results with the ones obtained while investigating the Twitter and Instagram profile, it is very likely that most of the users generated contents (textual or multimedia) are publicly accessible and contain geographical information.

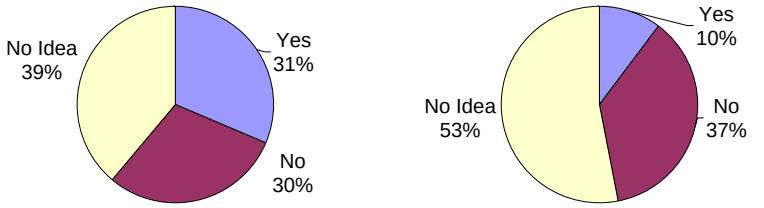

Fig. 11 Use of the geolocation feature on Twitter: men (left) and women (right).

To better understand the users' behavior, we investigate if the geolocation feature is used by people who claim to have selected the nature of their profile either private or public. Figure 13 reports the percentage of respondents who have a private profile and who claim to use the geolocation feature in Twitter (left) and Instagram (right). It can be observed that even among users with a private profile, the use of the geolocation feature is considerable (35% in Twitter and 43% in Instagram). Note the small percentage of people who have no idea.

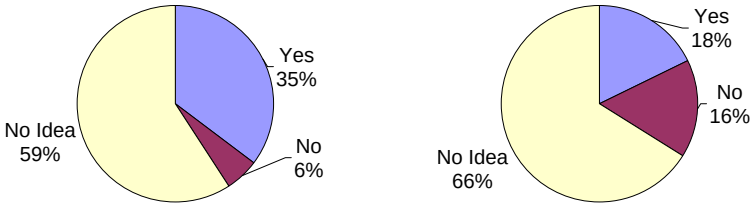

Fig. 12 Usage of the geolocation feature on Instagram: men (left) and women (right).

Figure 14 reports the percentage of respondents who have a public profile and who claim to use the geolocation feature in Twitter (left) and Instagram (right). It is interesting to note that 83% of of the Instagram users who selected their profile to public, claim to use the geolocation feature. It looks like people want to attach the geographical information to their generated contents. In particular, when sharing photos, people tend to attach geographical information to these contents.

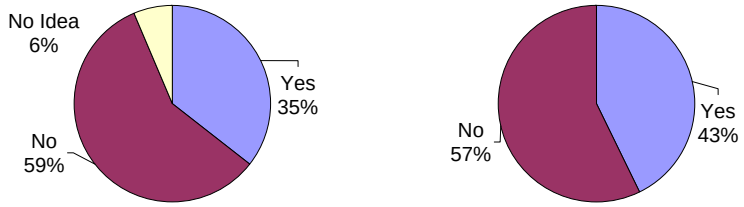

Fig. 13 Usage of the geolocation feature on Twitter (left) and Instagram (right) by considering people with a private profile.

The above results show that people ignore the way they share their generated contents and show that when they know, most of them attach the geographical information to their generated contents. What about privacy? Do people change privacy settings?

Figure 15 shows that people have no idea about privacy settings in Twitter: most of them (54% of men and 66% of women) do not remember changing the default privacy settings. A minority changed the privacy settings (22% of men and 16% of women) and the remaining did not (24% of men and 18% of women). Figure 16 shows the similar behavior also in the Instagram scenario.

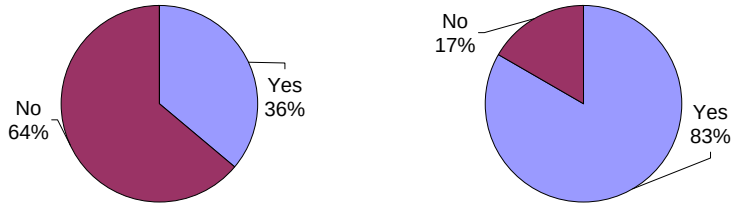

Fig. 14 Usage of the geolocation feature on Twitter (left) and Instagram (right) by considering people with a public profile.

According to these results, people are not concerned about privacy: the majority of them do not have idea about privacy settings and do not have idea about the nature of their profile. Moreover, half of the people who have idea about privacy settings or profile share their contents with everybody and use the geolocation feature. Again, this means that most of the users generated contents (textual or multimedia) are publicly accessible and contain geographical information.

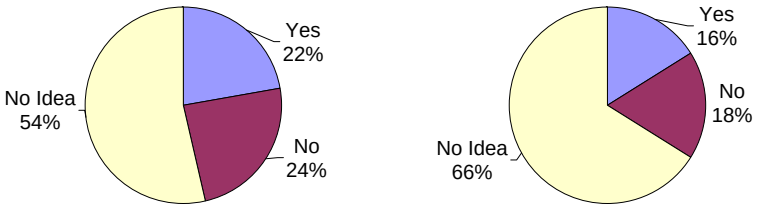

Fig. 15 Changes to privacy settings on Twitter: men (left) and women (right).

Among the ones who use the geolocation feature, we investigated the reasons of using this feature. Figure 17 reports the main users' motivations. People use the geolocation feature for a personal reason ("To remind me where I've been"): 51% in Instagram and 32% in Twitter. "To let others find my photos" has been checked by 32% of Instagram users and 22% of Twitter users. "To let my friends know where I am" is less popular: 14% in Instagram and 16% in Twitter. It is interesting to note that among the possible answers there was "To be contacted". None of the respondents checked this option.

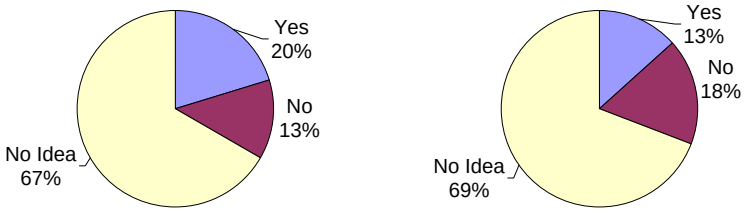

Fig. 16 Changes to privacy settings on Instagram: men (left) and women (right).

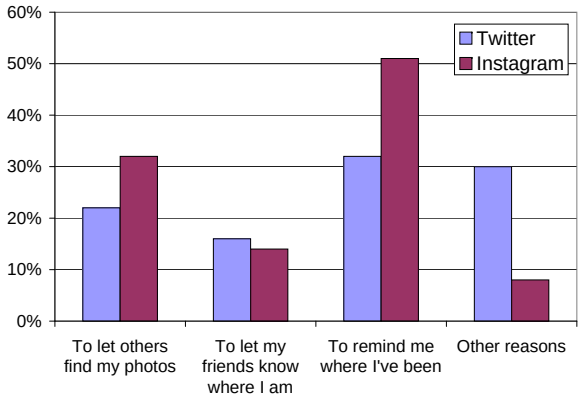

Fig. 17 Reasons to use the geo-localization feature on Twitter and Instagram.

3.3 Summary of Results

In this part of the investigation, we aimed at understanding if people are aware of the characteristics of the devices and applications they use. Based on the results we can say that a very large percentage of people own advanced devices, but have a lack of knowledge about the app scenario and about the way they publish contents into social platforms, as they do not know the type of profile they use and have no idea of privacy settings. Those who have a better knowledge decide to attach geographical information to their shared contents. Finally, among tweets and photos, people are more willing disseminate and share photos. In summary, the first part of the investigation depicts the following scenario.

- **Cellphone and connectivity**. Smartphones with GPS technology are widely available among participants and almost everyone is always connected to the Internet through flat-rate data plans. Hence, technology is not a burden for the development of an effective location-aware scenario;
- **Use of location-aware applications**. The majority of the respondents claim to use location-aware mobile applications. In the near future this

percentage is likely to increase due to the ever increasing availability of location-aware applications;
- **Twitter and Instagram presence**. The micro-blogging application is more popular than Instagram, but in both platforms users have no idea about the profile they use to publish their contents, nor they have about the usage of the geolocation feature (i.e., they do not know whether the application attaches user's location to the generated contents or not). This may represent a privacy risk for users;
- **Use of the geolocation feature**. Very personal reasons motivated users to enable the geolocation feature: "To remind me where I've been" is the main reason for using the geolocation feature, but other important reasons are related to user's friends ("To let others find my photos" and "To let my friends know where I am").

The high percentage of "don't remember", "don't know", "no idea" shows that a location-aware scenario is still an obscure entity for most of the users. To really understand users' opinions and preferences of this novel scenario, we think it is necessary to show them what third parties applications can do by browsing data in public social media platforms. To this aim, in the next section, we present details of an application we developed to create a location-aware scenario where users can be located in real-time and where personal information can be collected from public social media platforms. Once faced with the application, we will ask for users' opinions and preferences.

4 Location-aware scenario: an example

The real-world study presented in the previous section showed that people are not really concerned about privacy and largely use geolocation technologies. In this section, we show how to develop a simple application able extract personal and sensitive users information from contents publicly available in Twitter and Instagram and able to use these information to locate, in real-time, users on a map. Note that we focus our attention on the Twitter and Instagram platforms for two main reasons: i) it is possible to browse users' generated contents without signing up for the service, and ii) both platforms present a high volume of public data (no need to be friend to see someone's tweets or photos). Indeed, other applications, although popular like Foursquare and Facebook places, do not present a high volume of public data. However, it is worth mentioning that the application may be expanded to browse additional social media platforms if the corresponding APIs are available.

We recall here that the goal is to show that advanced skills or advanced technologies are not necessary and, therefore, anyone (your neighbor, your friends, your son, your parents, etc.) can exploit social platforms APIs to develop an application able to browse for geotagged contents and able to retrieve personal and sensitive information from each geotagged content.

To be as simple as possible, the application is developed with the following constraints:

- Use of **public data**. No need to sign-up to the social platforms to access to user's generated contents and no need to install the developed application on the users' device;
- Use of **real-time data**. The application exploits contents 'just' published by users so as to have an actual picture of the investigated scenario. Locating users in real-time can be very helpful in many scenarios, from emergency situation to media marketing;
- Use of **actual location**. The application does not infer or compute any user's location, but it relies on the location available in the metadata associated to user generated contents. Therefore, it is completely transparent to the geolocation technology used (i.e., Twitter and Instagram applications are in charge of attaching geo-coordinates to the user generated contents).

In the following, we present details of the application development and of the application output.

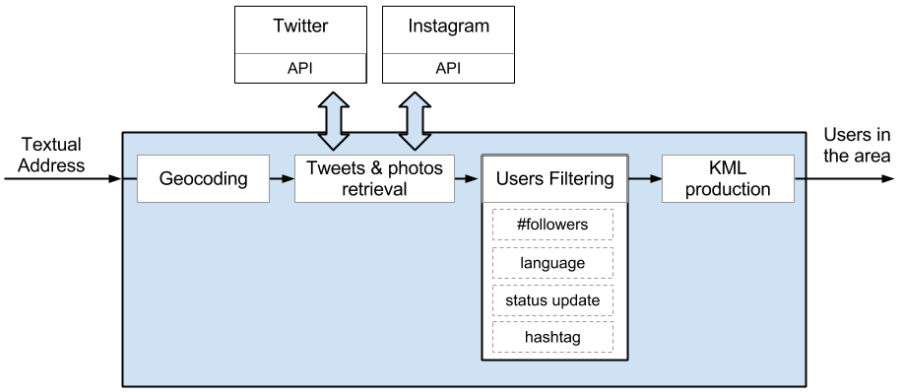

Fig. 18 The architecture of the application designed to create a location-aware scenario.

4.1 Application Development

The application is developed with Python 2.7[2] and, as depicted in Figure 18, is logically organized into four main blocks: i) Geocoding, ii) Tweets and photos Retrieval, iii) Users Filtering, and iv) KML production.

Geocoding
This module converts an address provided in a textual form (street and city

[2] Python Programming Language Official Website: http://www.python.org/

Description	API Field
Geographical coordinatees	coordinates
Creation time	created_at
ID	id_str
Number of times the Tweet has been retweeted	retweet_count
The actual text	text
Author	user

Table 1 Some of the fields associated to a single tweet.

name) into its GPS coordinates (latitude and longitude) so as to allow the "Tweets and photos retrieval" module to look for contents produced in the area. The application uses the geopy library[3] to convert a textual address (street name and city) into its GPS coordinates. For instance, by entering our department address we have the following coordinates:

Viale Allegri 9, Reggio Emilia, Italy → (44.70304, 10.62957).

Tweets and photos retrieval

The application directly interacts with Twitter and Instagram platforms through the platforms' API[4][5]. In this way, it is possible to browse and access to public data in their platforms. In addition to the user generated contents, it is possible to access to the metadata associated to the content. For instance, when accessing to a single tweet, it is possible to know the geographical location and the time the tweet has been written, the number of times the tweet has been retweeted and the tweet author (see, Table 1). By knowing the tweet author, it is possible to retrieve several personal user information: for instance, among the several information available, it is possible to know the account creation time, how the author describes him/herself, the number of followers (and their names), the number of friends (and their names), the preferred language, the author's photo, etc. (see, Table 2). Similarly, starting from an Instagram photo, it is possible to obtain several information about the photo and about its author (see, Table 3 and Table 4).

Twitter and Instagram provide APIs that allow searching for tweets/photos by specifying longitude and latitude. The APIs return the contents (in JSON, JavaScript Object Notation format) generated by users located within a given radius of the given geographical coordinates. For instance, if we want to look for contents produced not more than 2 miles from our department, the APIs require the triplet (44.70304, 10.62957, 2mi). The result is a list of contents (tweets or photos) coupled with several personal and sensitive information about the users who generated the contents.

[3] http://code.google.com/p/geopy/
[4] Twitter API: https://dev.twitter.com/
[5] Instagram API: http://instagram.com/developer/

Description	API Field
Account creation time	created_at
Account description	description
Number of followers	followers_count
Number of followings	friends_count
User interface language	lang
User location	location
User name	name
User screen name	screen_name
The user's most recent tweet or retweet	Status
The number of issued tweets (including retweets)	user statuses_count

Table 2 Some of the fields associated to a Twitter user.

Description	API Field
Photo description	media.caption
Hashtag	media.tags
Number of received likes	media.like_count
Number of received comments	media.comment_count
Geographical coordinates location	media.location.point
Photo publication time	media.created_time
Photo URL	media.images.url

Table 3 Some of the fields associated to an Instagram photo.

Description	API Field
Name	media.user.full_name
Nickname	media.user.user_name
ID	media.user.id
Description	Media.user.bio
URL	Media.user.website

Table 4 Some of the fields associated to an Instagram user.

Users Filtering

The list of users produced by the previous module contains all the Twitter and Instagram users that are located in a specific area and every user is described with personal and sensitive information. The number of such users may be very high (think of users located in Time Square, NYC) and may be composed of users with very different characteristics (e.g., languages, number of followers, etc.). In addition to the no-filter option, this module allows filtering users in four different ways: number of followers, user language, number of generated contents, keyword within tweet or photo description. Therefore, for a given area, it is possible to locate popular users (by filtering them according to the number of followers), or users who speak a specific language (by filtering them according to the language), or users who wrote more tweets or shoot more photos (by filtering them according to the number of generated contents), or users who wrote tweets or described photos

with a particular keyword. In essence, the module selects a set of users (each one described with personal and sensitive data) located in a specific area.

KML Production
To display the selected set of users on a map, we consider the KML (Keyhole Markup Language) format [20], an international standard of the Open Geospatial Consortium. This format is widely supported by the most common geospatial tools and web mapping services (e.g., Google Maps and Google Earth). It is XML-based and is designed to attach visualization details and metadata to geo-reference media resources. Furthermore, it offers a rich set of options to visualize objects within 2D and 3D maps.

Table 5 shows an example of a KML description. Every user located in a specific area is described through the `placemark` tags. Every placemark is associated to a specific geographical point (through the tags `coordinates`), has a name (through the tag `name`) and may contain a description (through the tag `description`) which is a generic container that can be filled with any textual information. It is to note that KML supports the HTML-encoded description within the `description` tag.

The module generates the KML file by describing every users selected by the previous module within `placemark` tags: the GPS coordinates are described through the `coordinates` tags and all the personal and sensitive information are described in HTML format (for easier reading when displayed on a map) and inserted between `<description>...</description>` tags.

4.2 Application Input/Output

The application is developed to show that anyone can exploit social platforms APIs to develop a program able to browse for geotagged contents (i.e., for contents generated in a specific neighborhood) and able to retrieve personal and sensitive information from each geotagged contents. It has a textual interface and requires: an address, the radius where to search for users and the filtering options (see User Filtering Module). After receiving these data, the application produces a KML file that can be visualized with maps tools like Google maps and Google Earth.

Figure 19 shows how Google Earth displays KML file produced by the developed application: all the users located in the specific area (Piazza Maggiore, Bologna, Italy) are described through yellow pins and when a specific user is selected, the retrieved information about the user are displayed. Figure 20 shows an example of the personal information that can be collected through public browsing of the Twitter/Instagram platform: in addition to the user name and name account, it is possible to know the account creation time (June 24, 2009), the interface language (English), the user picture, the personal URL where to find additional and personal information, the user description as written by the user, the usual location (Paris), the number

```
<?xml version="1.0" encoding="UTF-8"?>
<kml xmlns:gx="http://www.google.com/kml/ext/2.2"
         xmlns:atom="http://www.w3.org/2005/Atom"
         xmlns="http://www.opengis.net/kml/2.2">
  <Folder>
    <Placemark>
      <name>USER NAME</name>
      <description>GENERIC TEXTUAL DESCRIPTION</description>
      <Point>
        <coordinates>GEO COORDINATES</coordinates>
      </Point>
    </Placemark>
     ...
  </Folder>
</kml>
```

Table 5 KML description: every user is described within a placemark.

of followers and the number following, the last written text and its creation time.

By looking at these data, we can identify this user as a woman who lives in Paris and works as a photographer and travelblogger. We also know she is co-founder of a travel association, she has a considerable number of followers and she follows a considerable number of people. Furthermore, from her description we also know her Facebook account. Needless to say, we also know she was in Galleria Cavour (a shopping center near Piazza Maggiore square in Bologna) when we checked the area (on July 11, 2013).

Figure 21 shows the same output of Figure 19 but displayed with Google Maps.

5 Location-aware scenario: opinions and preferences

In the previous section, we showed that a simple application may access to personal and sensitive data without asking for permission and without logging-in into the social platforms. Indeed, in an anonymous way, third parties may browse social platforms and may retrieve users' personal and sensitive information. In the near future, it is likely that organizations and industries will exploit public metadata with geolocation data to create services we have not yet considered.

To investigate if users are aware of possible privacy and security risks when using location-aware applications, we showed to the same participants of Section 3 the location-aware scenario described in the previous section and then we submitted them a questionnaire to understand their opinions and preferences.

The first question was: "What would be your reaction if third parties would access to your physical location through specific technologies without

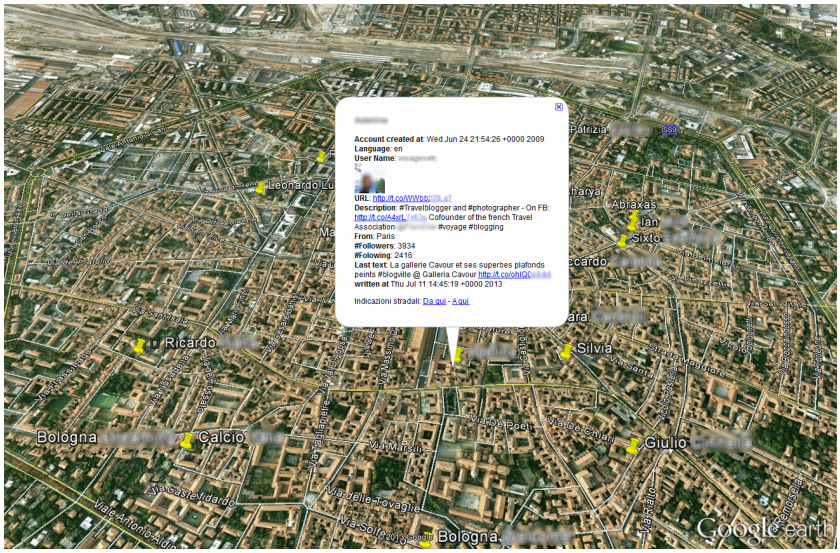

Fig. 19 The set of users located in a specific area as displayed in Google Earth. Every user is described with several personal information. Note that sensitive personal information have been partially obscured for privacy reasons.

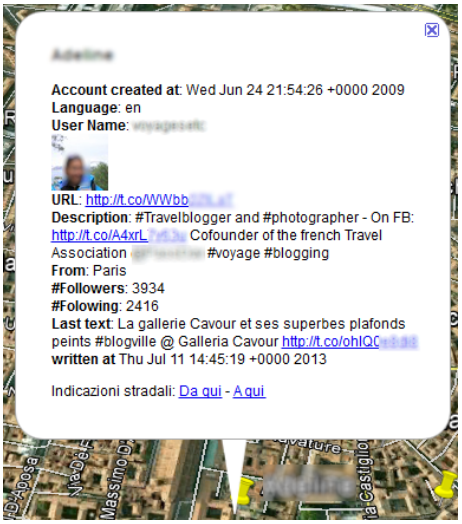

Fig. 20 Details of a user located in the area. Note that sensitive personal information have been partially obscured for privacy reasons.

asking for your authorization?". Answers were: "Discomfort", "Indifferent", "Angry", "I would think about personal benefits" and "I would think about negative consequences". Multiple checks were possible.

Figure 22 reports the obtained reactions when considering people who claim to use location-aware applications and people who do not. We can ob-

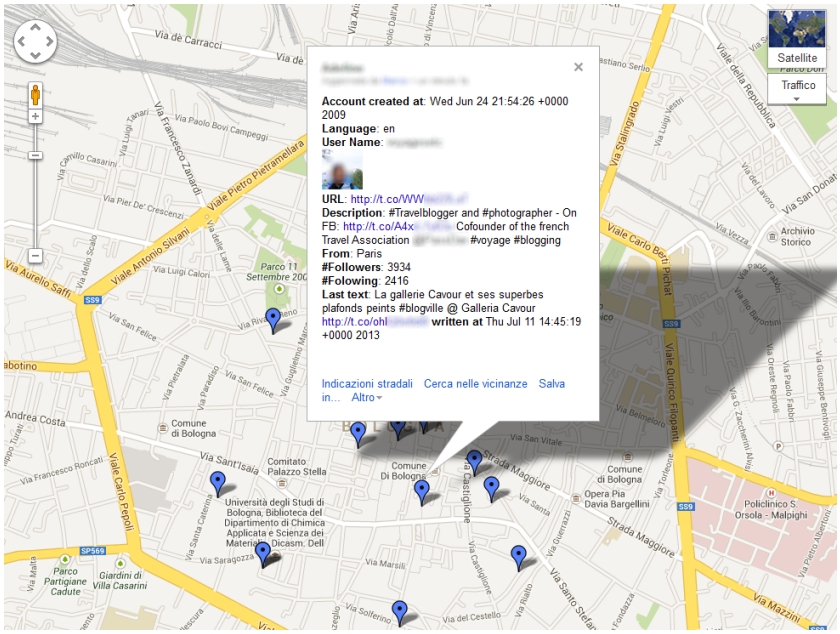

Fig. 21 The set of users located in a specific area as displayed in Google maps. Every user is described with several personal information. Note that sensitive personal information have been partially obscured for privacy reasons.

serve that people who do not use location-aware applications (left) are more worried than people who claim to use location-aware applications (right): more "angry" answers (23% vs. 17% among men, and 47% vs. 20% among women), more "discomfort" (54% vs. 28% among men, and 47% vs. 34% among women) and more "think about negative consequences" (38% vs. 14% among men, and 63% vs. 37% among women).

The reactions show that people are not really aware of what can happen when personal location is embedded into user generated contents shared in public platforms. In particular, the analysis highlights that women are more worried than men about the scenario. In general, results show that people who use location-aware applications are less worried about third parties accessing personal location.

To understand if there are different reactions among Twitter and Instagram users, in the following we analyze users' reactions according to personal profile (private, public or no idea) and to privacy settings (changed, not changed or no idea).

Figure 23 reports the reactions of Twitter users. Results show that men have similar reactions regardless of their profile type and of possible changes to their privacy settings, whereas women behave differently. Women with a private profile and women who changed their privacy settings think about possible personal benefits. Likely, these women use privacy settings tools

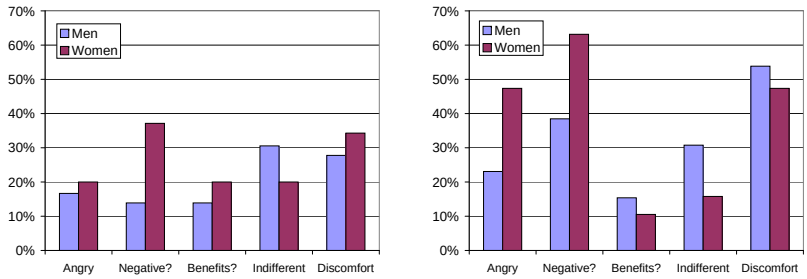

Fig. 22 Users' opinion when asking: "What would be your reactions if third parties would access to your physical location through specific technologies without asking for your authorization?". People who claim to use location-aware applications (left) and people who claim not to use location-aware applications (right).

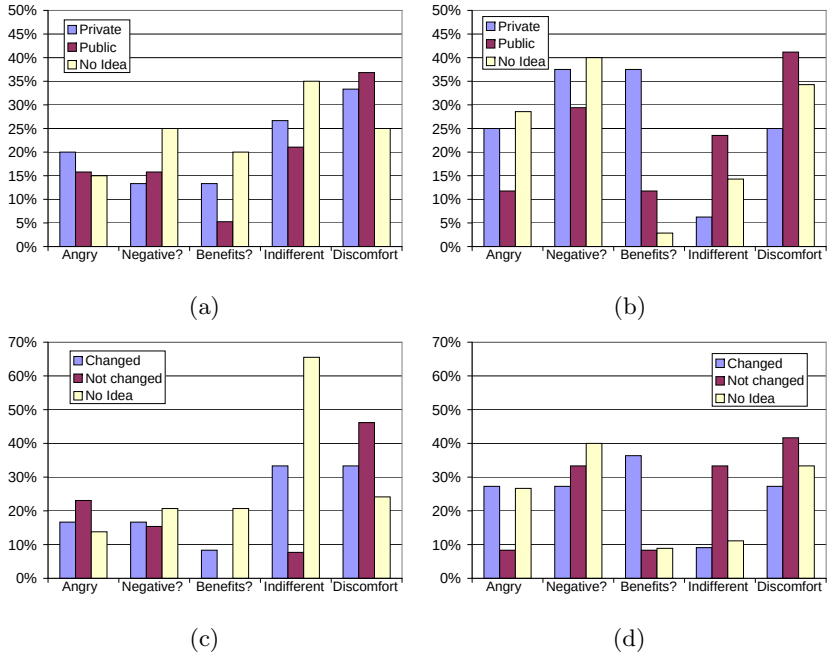

Fig. 23 Twitter users' opinion when asking: "What would be your reactions if third parties would access to your physical location through specific technologies without asking for your authorization?": men (a-c) and women (b-d).

to protect their contents and therefore they are not worried about third parties accessing to their personal locations. Not being worried, they think of possible benefits.

In particular, Figure 23 (a) we report men reactions according to personal profile: men with a private profile feel "discomfort" (33%) or "indifference" (27%); reactions are similar for men with a public profile: "dis-

comfort" (37%) and "indifference" (37%); reactions are slightly different for men who have no idea about their profile: "indifferent" (35%) and "think about negative consequences" (25%). Figure 23 (b) reports women reactions according to personal profile and shows that among women, users with a private profile "think about negative consequences" or "personal benefits" (37%); users with a public profile feel "discomfort" (41%) or "think about negative consequences" (29%), and users who have no idea about their profile "think about negative consequences" (40%) and feel "discomfort" (34%). In Figure 23 (c) we report men reactions according to privacy settings: men who changed privacy settings feel "discomfort" or are "indifferent" (33%); men who did not change their privacy settings feel "discomfort" (46%) or are "angry" (23%) and men who have no idea about changing their privacy settings are "indifferent" (65%). Among women (Figure 23 (d)), users who changed privacy settings think about "personal benefits" (36%); users who did not change privacy settings feel "discomfort" (42%) and users who have no idea about changing their privacy settings "think about negative consequences" (40%).

Figure 24 reports the reactions of Instagram users. Looking at the results, we observe that people (either men or women) are angry (or think about negative consequences) if third parties would access to their photos, regardless of profile type or privacy settings changes. It is interesting to note that a considerable percentage of men with private or public profile and of men who changed their privacy settings are "indifferent"; also, it is interesting to observe that a considerable percentage of women with a public profile think about personal benefits. With respect to the Twitter scenario, reactions of Instagram users are more negative and settled. Likely, photos are considered more personal than tweets and, therefore, if third parties access to personal location through photos, users feel like an invasion of their privacy.

In particular, Figure 24 (a) reports men's reactions according to personal profile: men with a private profile are "angry" (43%), "indifferent" (29%) or feel "discomfort" (29%); men with a public profile are "indifferent" (33%) and men who have no idea about their profile feel "discomfort" (41%). Note that none of them think about personal benefits. Figure 24 (b) reports women's reactions according to personal profile and shows that among women, users with a private profile "think about negative consequences" (57%) or are "angry" (43%); users with a public profile "think about negative consequences" (47%), feel "discomfort" (33%) and think about "personal benefits" (27%); users who have no idea about their profile feel "discomfort" (39%) and "think of negative consequences" (30%). Figure 24 (c) reports men's reactions according to privacy settings: men who changed privacy settings are "indifferent" (45%) or "angry" (36%); men who did not change their privacy settings feel "discomfort", are "angry" and "think about negative consequences" (29%); men who have no idea about changing their privacy settings feel "discomfort" (40%). Figure 24 (d) reports women's reactions according to privacy settings: among women,

users who changed privacy settings are “angry” (56%) or “think about negative consequences” (44%); users who did no change privacy settings “think about negative consequences” (50%) and users who have no idea about changing their privacy settings feel “discomfort” (38%) or “think about negative consequences” (32%).

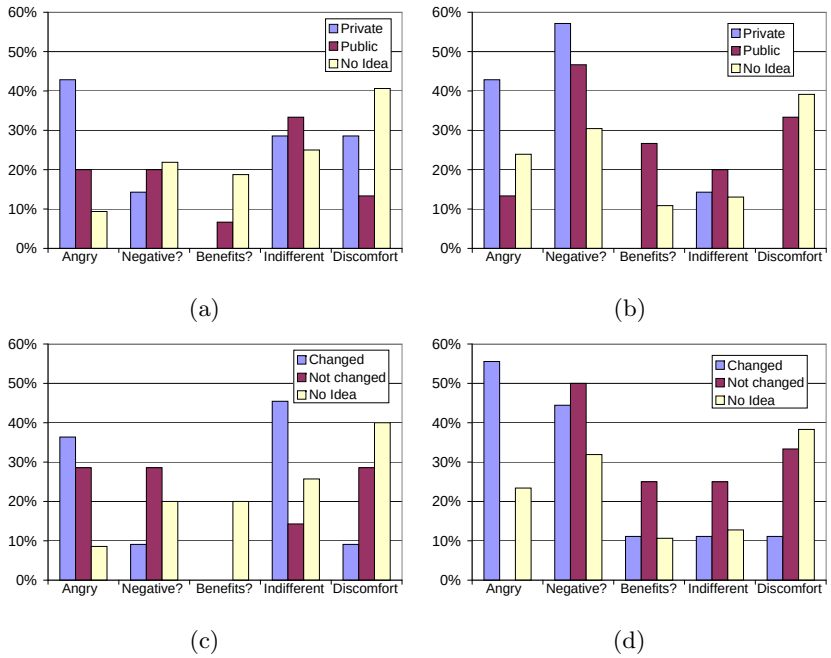

Fig. 24 Instagram users’ opinion when asking: “What would be your reactions if third parties would access to your physical location through specific technologies without asking for your authorization?”: men (a-c) and women (b-d).

The second question was: “Would you like to be contacted by third parties according to the location of your tweets or photos?”. Possible options were: “Yes”, “Yes, after my authorization”, “Yes, if messages are not numerous”, “Yes, if I can receive benefits”, “Yes, but just for marketing reasons”, “Yes, but not marketing reasons”, “Yes, If I can be of any help to someone else” and “No”. Multiple choices were possible.

Figure 25 reports the obtained results when considering people who claim to use location-aware applications and people who do not. The most checked option was “No”, regardless users are familiar with location-aware applications or not. However, the number of people who are willing to be contacted is considerable, provided some constraints are met. In particular, the authorization seems to be mandatory for people who use location-aware applications and another important reason is to receive benefits (either personal or for someone else) from the service. According to these results, a

third-party service that requires authorization before accessing to personal data and provides benefits may become popular among users.

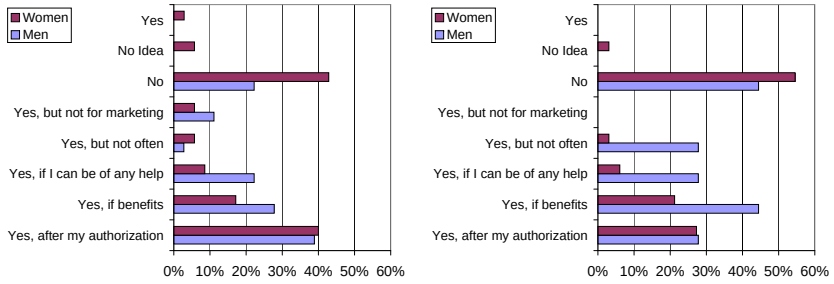

Fig. 25 Users' opinion when asking: "Would you like to be contacted by third parties according to the location of your tweets or photos?" People who claim to use location-aware applications (left) and people who claim not to use location-aware applications (right).

To understand if there are different opinions among Twitter and Instagram users, in the following we analyze users' opinions according to personal profile (private, public or no idea) and to privacy settings (changed, not changed or no idea).

Figure 26 reports the opinions of the Twitter users. Results show that people (either men or women) who ignore the nature of their profile respond in a defensive manner and do not like to be contacted; conversely, people who know their type of profile are more confident and would like to enter the location-aware scenario provided some constraints are met: give authorization and receive benefits.

In particular, Figure 26 (a) reports men's opinions according to personal profile: men with private and public profile require third parties to be authorized (47% and 32%, respectively); men with private profile think also about personal benefits (27%) and benefits of others (33%). Conversely, men with no idea about their profile do not like to be contacted by third parties (40%). Figure 26 (b) reports women's opinions according to personal profile: women with private profile do not like to be contacted (32%) or require third parties to be authorized (32%); women with public profile require third parties to be authorized (58%). Conversely, women with no idea about the type of their profile do no like to be contacted (60%). Figure 26 (c) reports men reactions according to privacy settings: men who changed their privacy settings do not like to be contacted (67%) or require third parties to be authorized (38%). Men who did not change their privacy settings require third parties to be authorized (39%). Similarly, men with no idea privacy settings, require third parties to be authorized (39%). Figure 26 (d) reports women reactions according to privacy settings: women who have no idea about modification to their privacy settings do not like to be

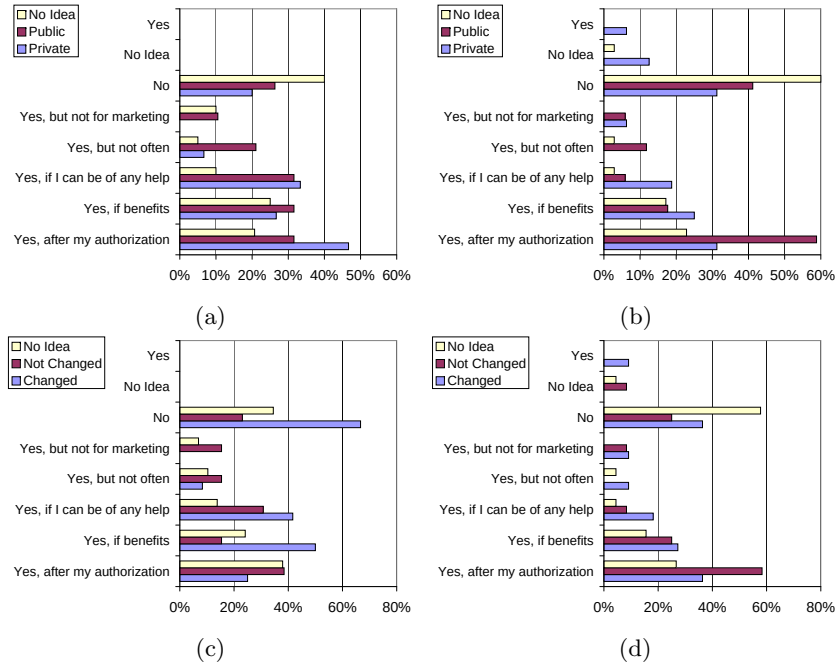

Fig. 26 Twitter users' opinion when asking: "Would you like to be contacted by third parties according to the location of your tweets or photos?": men (a-c) and women (b-d).

contacted (58%); women are willing to be contacted if there is an authorization process (58% of who did not change their privacy settings and 36% of who changed their privacy settings).

Figure 27 reports the opinions of the Instagram users. Results show that men who have no idea about their profile or about changing their privacy settings do not like to be contacted or require third parties to be authorized; similarly, men who have idea about their profile and men who changed their privacy settings do not like to be contacted; however, they also think about benefits (either personal or not) and would require authorization for third parties. Women with a private profile and women who changed their privacy settings do not like to be contacted. Likely, they changed their privacy settings in order to protect their photos and not to be disturbed. Among the ones who have no idea about their profile or set their profile as public, provide authorization is an option for being contacted. With respect to the Twitter scenario, people tend to be more protective. It looks like, photos are more private than tweets. Women are willing to be contacted by third parties when using Twitter, but when using Instagram they absolutely do not want to be contacted. For men, it looks like the opposite: men who share photos are more willing to be contacted than men who share tweets.

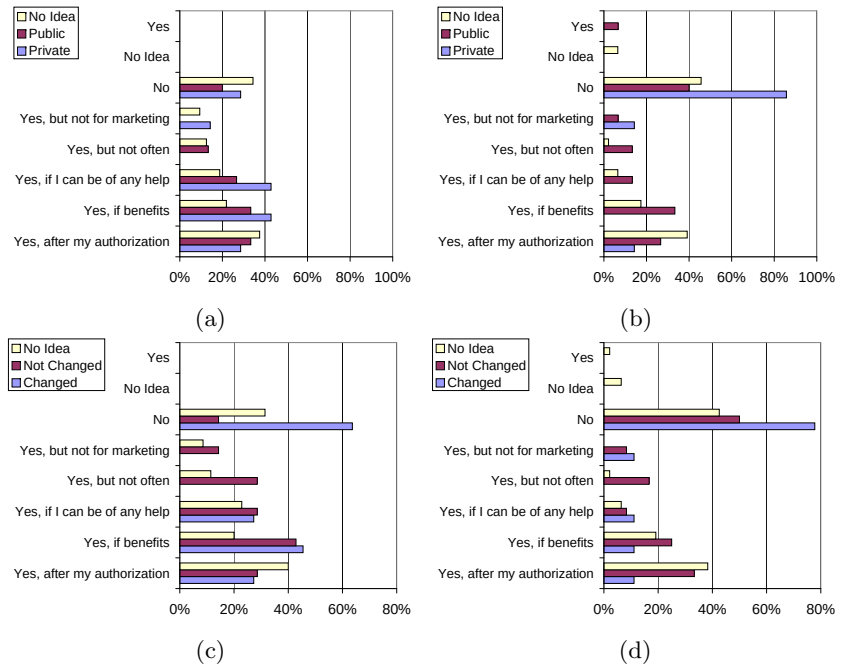

Fig. 27 Instagram users' opinion when asking: "Would you like to be contacted by third parties according to the location of your tweets or photos?": men (a-c) and women (b-d)

In particular, Figure 27 (a) reports men's opinions according to personal profile: men who have a private profile are willing to be contacted provided there are benefits, either personal or for others (43%). Similarly, men who have a public profile are willing to be contacted if there is an authorization process (33%), if there are personal benefits (33%) or if there are benefits for someone else (27%). The situation is different when considering people who have no idea about their profile: 34% do not like to be contacted and 38% are willing provided third parties are authorized. Figure 27 (b) reports women's opinions according to personal profile: women who have no idea about their profile do not like to be contacted (46%) and think about requiring third parties to be authorized (39%); women who have a private profile do not like to contacted (86%), and women who have a public profile do not like to be contacted (40%) or think about personal benefits (33%). Figure 27 (c) reports men reactions according to privacy settings: men who changed their privacy settings do not like to be contacted (64%) or require third parties to provide benefits (45%); men who did not change their privacy settings require third parties to provide benefits (43%), to ask for an authorization (29%), to provide benefits to someone else (29%), and men with no idea about privacy settings, require third parties to be authorized (40%) or do not like to be contacted (31%). Figure 27 (d) reports women reactions according

to privacy settings: women who changed their privacy settings do not like to be contacted (78%); women who did not changed privacy settings do not like to be contacted (50%) or require third parties to be authorized (33%), and women who have no idea about changing their privacy settings do not like to be contacted (43%) or require third parties to be authorized (38%).

Finally, we asked participants "How would you define a service able to contact you according to the geographical area embedded in your tweets or photos?". Possible options were: "Advantageous", "Alarming", "Useful", "Negligible", "Interesting", "Intrusive". Multiple choices were possible.

Figure 28 reports the obtained results when considering people who claim to use location-aware applications and people who do not. In general, there is no great difference between the two groups of people. The number of people who define the service as "Intrusive" is greater among the ones who do not use location-aware applications; similarly, the number of people who define the service as "Interesting" is greater among the ones who use location-aware applications. Another interesting difference regards the "Alarming" adjective: women who use location-aware applications are more worried than women who do not use such applications (20% vs. 9%). Likely, women do not have a clear idea of what information a location-aware application can publish over social platforms and once they realized what it is possible to do (through the location-aware scenario showed in Section 4), they define the service as alarming.

To understand if there are different definitions among Twitter and Instagram users, in the following we analyze users' definitions according to personal profile (private, public or no idea) and to privacy settings (changed, not changed or no idea).

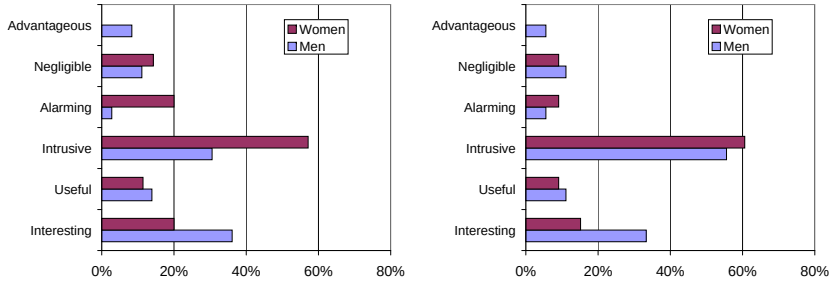

Fig. 28 Users' opinion when asking: "How would you define a service able to contact you according to the geographical area they specified in their tweets or photos?" People who claim to use location-aware applications (left) and people who claim not to use location-aware applications (right).

Figure 29 reports the definitions of the Twitter users. Men who know their profile, as well as men who changed their privacy settings, define the service as "Interesting", otherwise the service is defined as "Intrusive".

Women define the service as "Intrusive" regardless the type of profile they have or the changes to privacy settings they made. When defining the service, women are less interested and more alarmed than men.

In particular, in Figure 29 (a) we report men's definitions according to personal profile: men with private profile define the service as "Interesting" (40%); 42% of men with a public profile define the service as "Intrusive", but the same percentage of people define the service as "Interesting". Men who have no idea about their personal profile define the service as "Intrusive" (50%). Figure 29 (b) reports women's definitions according to personal profile: women define the service as "Intrusive" regardless of the type of profile they have. Women with a private profile define the service as "Interesting" (27%). Figure 29 (c) reports men's definitions according to privacy settings: among men who changed their privacy settings, the service is defined as "Interesting (50%). Among the ones who did not change or did not remember changing privacy setting, the service is defined as "Intrusive" (54% and 38%, respectively). However, it is interesting to note that the "Interesting" definition achieves considerable percentages among people who did not or do not remember changing privacy settings. Figure 29 (d) reports women's definitions according to privacy settings: women define the service as "Intrusive" regardless of wheter they changed privacy settings or not.

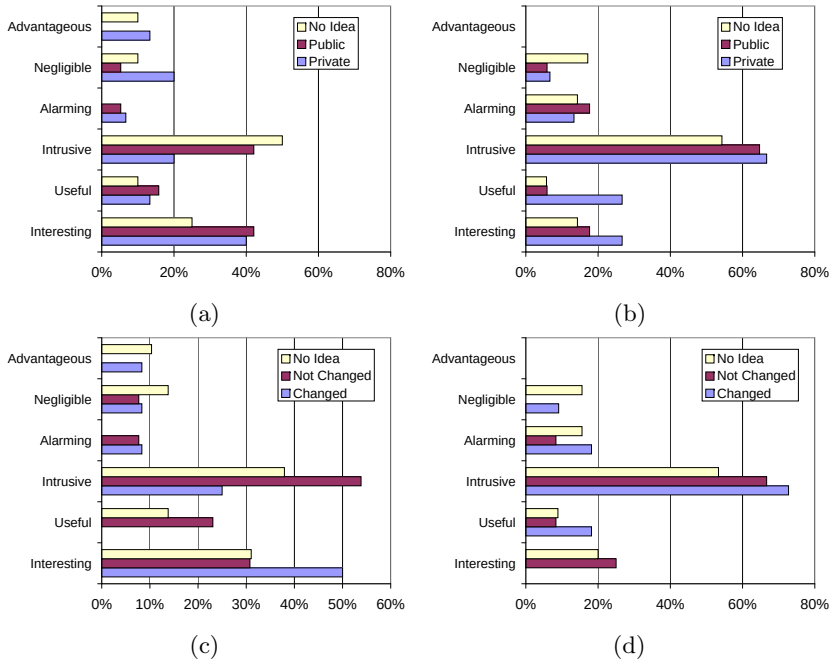

Fig. 29 Twitter users' opinion when asking: "How would you define a service able to contact you according to the geographical area specified in your tweets?": men (a-c) and women (b-d).

Figure 30 reports the definitions of the Instagram users. Results show that men define the service as "Intrusive" if they have no idea about privacy settings or profile type, otherwise the service is defined as "Interesting". Among women, the service is defined as "Intrusive".

In particular, Figure 30 (a) reports men's definitions according to personal profile: men who have no idea about their profile define the service as "Intrusive" (50%), the others define the service as "Interesting" (29% and 60% for the ones with private and public profile, respectively). Figure 30 (b) reports women's definitions according to personal profile: women define the service as "Intrusive" and only 29% of women with a private profile define the service as "Interesting". Figure 30 (c) reports men's definitions according to privacy settings: men who have no idea about privacy settings define the service as "Intrusive" (46%), the others define the service as "Interesting" (36% and 57% for the ones with private and public profile, respectively) Figure 30 (d) reports women's definitions according to privacy settings: women define the service as "Intrusive" and only 25% of women who did not change their privacy settings define the service as "Interesting".

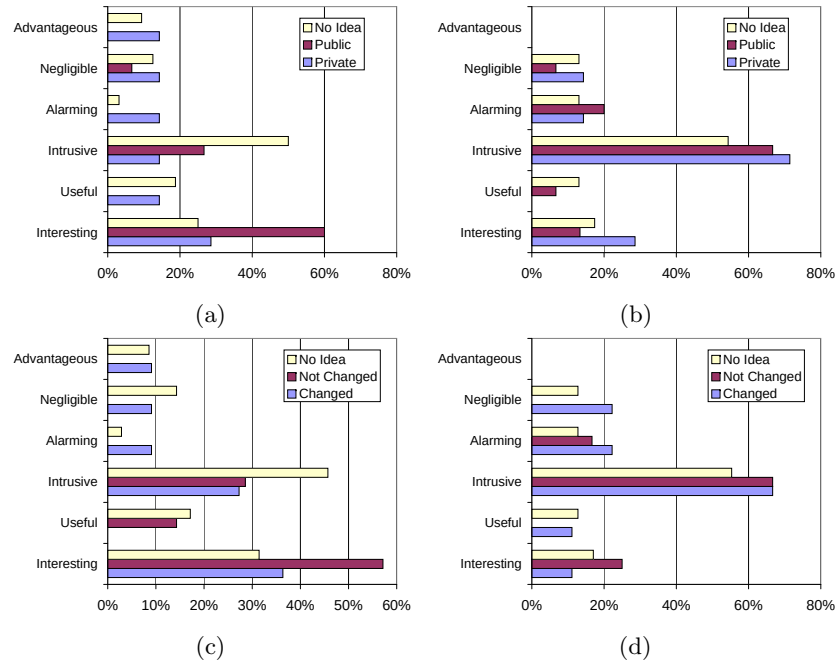

Fig. 30 Instagram users' opinion when asking: "How would you define a service able to contact you according to the geographical area specified in your photos?": men (a-c) and women (b-d).

5.1 Summary of Results

The second part of the investigation aimed at understanding users' opinions and preferences about a location-aware scenario after seeing what a simple application can do by browsing data publicly available in social platforms. Results showed that people who were initially not concerned about privacy, resulted to be the most worried about the location-aware scenario; conversely, people who were initially concerned resulted to be less worried about the location-aware scenario and found the scenario interesting. Therefore, the two-phase analysis showed that there is an implication between public location information and users' awareness: people who have no idea about personal profile or privacy settings are not willing to enter into a location-aware scenario as they define the service as "Intrusive". Conversely, people who do have idea about personal profile or privacy settings are willing to enter into a location-aware scenario provided some constraints are met. In particular, give authorization to third parties and receive benefits seem to be the mandatory constraints to realize a location-aware scenario.

In summary, the second phase of the investigation depicts the following scenario.

- **Users' reaction**. Users of location-aware applications are less worried than those who do not use location-aware applications. Women seem to be more worried than men. When talking about photo the "angry" reaction is predominant.
- **Users' will to be contacted**. People do not like to be contacted, but if the service asks for their authorization and if it provides benefits, users are willing to be contacted.
- **User's opinions**. Men find the service "Interesting", whereas women find it "Intrusive".

Although the majority of the participants negatively defined the service, several positive opinions were checked. If on the one side users are worried about the usage of public data to locate and contact them, on the other side they did not have preconceived ideas about a location-aware scenario. Indeed, according to the obtained results, users are willing to enter into a location-aware scenario if there are clear rules and benefits.

6 Guidelines for developing an effective location-aware scenario

Results showed that technology is not a burden for the development of an effective location-aware scenario, but also highlighted that users are not completely aware of what happens in the mobile scenario when producing or sharing contents. Furthermore, results also showed that, after showing users the amount of personal and sensitive data that can be extracted from contents publicly available in social platforms, the majority of people thought about possible negative consequences and, in general, the concerns about

privacy have grown. Needless to say, these concerns may hinder the success of the location-aware scenario. In the following, we propose some guidelines for both users and developers/enterprises that might be helpful in developing an effective location-aware scenario.

From the developers/enterprises point of view, a successful location-aware scenario will provide a better knowledge of their customers (e.g, urban movements, timetable, etc), will provide users with a better service (e.g., developed according to users' habits), will allow designing more efficient advertising campaign (e.g., place advertising signs in areas highly frequented by potential customers), will provide customization services (e.g., video on demand according to users' location) and will introduce novel services (e.g., the use of geo-reference data combined with the Internet may facilitate the success of the augmented reality.) However, to build an effective location-aware scenario, developers/enterprises should be aware that users do not want to be bothered for marketing or advertisement reasons. Instead, users are willing to enter into a location-aware scenario if services will ask for their authorization before accessing to their personal data and if they provide benefits to them. Developers/enterprises should also be aware that users consider photos a more private resource than tweets. Moreover, since in current OSs, the process of enabling/disabling the geolocation technologies is not straightforward, the developed application should aware users when they are sharing contents with personal data hidden in the shared resource. Similarly to the message that pops-up the first time the device tries to go on-line ("Continuing Internet access will lead to traffic. Continue?"), applications should aware users of what personal data are going to be shared in social platforms. For instance, a message like "The photo you are sharing allows third parties to locate you" allowing users to select between two possible options "Remove geolocation info" or "Continue" would be very informative for the users.

From the user point of view, a successful location-aware scenario will facilitate many aspects of their lives, but it will also represent a risk for their privacy. Technology can help to protect users' privacy, but users have a key role in protecting their data. For this reason, users should be aware of the technologies available in their device and should know advantages and disadvantages of using these technologies; should know how to enable/disable specific services and/or technologies, should be aware of what data the installed applications have access to, should be aware that multimedia content (either photos or videos) are usually coupled with a lot of personal and sensitive information, and, needless to say, they should know what data are fundamental/critical for the applications.

7 Conclusions

In this paper, we investigated attitudes, behaviors and opinions of users with respect to the location-aware scenario. The investigation was done

in two phases: the first phase aimed at understanding what people know or ignore of a location-aware scenario and the second phase investigated users' opinions after showing them the amount of personal and sensitive information that a simple application can access to by browsing contents publicly available in social media platforms.

Results showed that people who are not initially concerned about privacy are the most worried about the location-aware scenario; conversely, people who were initially concerned, are less worried about the location-aware scenario and find the scenario interesting. Results also showed that men are more willing than women to enter the location-aware scenario, but both require to give authorization and to receive benefits when third parties access to their contents. Other interesting findings were that users do not want to be bothered with marketing or advertising services, that women are very alarmed if third parties would access to their photos and that photos are considered as a personal resource that need to be protected from third parties access.

The analysis of the obtained results allowed us to outline possible guidelines that we think might be helpful for both users and developers/enterprises to build an effective location-aware scenario.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper.

References

1. H. Li, H. Hu, and J. Xu. Nearby friend alert: Location anonymity in mobile geo-social networks. *Pervasive Computing, IEEE*, PP(99):1, 2012.
2. Stefano Ferretti, Marco Furini, Claudio E. Palazzi, Marco Roccetti, and Paola Salomoni. WWW recycling for a better world. *Communication of the ACM*, 53(4):139–143, April 2010.
3. Tom Leighton. Improving performance on the internet. *Commun. ACM*, 52(2):44–51, February 2009.
4. Yu Zheng, Lizhu Zhang, Xing Xie, and Wei-Ying Ma. Mining interesting locations and travel sequences from gps trajectories. In *Proceedings of the 18th international conference on World wide web*, WWW '09, pages 791–800, New York, NY, USA, 2009. ACM.
5. Eunjoon Cho, Seth A. Myers, and Jure Leskovec. Friendship and mobility: user movement in location-based social networks. In *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining*, KDD '11, pages 1082–1090, New York, NY, USA, 2011. ACM.
6. Lars Backstrom, Eric Sun, and Cameron Marlow. Find me if you can: improving geographical prediction with social and spatial proximity. In *Proceedings of the 19th international conference on World wide web*, WWW '10, pages 61–70, New York, NY, USA, 2010. ACM.

7. Rui Li, Shengjie Wang, Hongbo Deng, Rui Wang, and Kevin Chen-Chuan Chang. Towards social user profiling: unified and discriminative influence model for inferring home locations. In *Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining*, KDD '12, pages 1023–1031, New York, NY, USA, 2012. ACM.
8. Zhiyuan Cheng, James Caverlee, and Kyumin Lee. You are where you tweet: a content-based approach to geo-locating twitter users. In *Proceedings of the 19th ACM international conference on Information and knowledge management*, CIKM '10, pages 759–768, New York, NY, USA, 2010. ACM.
9. Gerald Friedland, Oriol Vinyals, and Trevor Darrell. Multimodal location estimation. In *Proceedings of the international conference on Multimedia*, MM '10, pages 1245–1252, New York, NY, USA, 2010. ACM.
10. Marco Roccetti, Stefano Ferretti, Claudio E. Palazzi, Marco Furini, and Paola Salomoni. Riding the web evolution: from egoism to altruism. In *Proceedings of the IEEE Consumer Communication & Networking 2008 (CCNC2008)*, pages 1123–1127, January 2008.
11. ISACA. Geolocation: Risk, issues and strategies. Technical report, 2011.
12. Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. Location disclosure to social relations: why, when, & what people want to share. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '05, pages 81–90, New York, NY, USA, 2005. ACM.
13. Patrick Gage Kelley, Michael Benisch, Lorrie Faith Cranor, and Norman Sadeh. When are users comfortable sharing locations with advertisers? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, pages 2449–2452, New York, NY, USA, 2011. ACM.
14. Erika Chin, Adrienne Porter Felt, Vyas Sekar, and David Wagner. Measuring user confidence in smartphone security and privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 1:1–1:16, New York, NY, USA, 2012. ACM.
15. Gamhewage C. de Silva and Kiyoharu Aizawa. Interacting with location-based multimedia using sketches. In *Proceedings of the ACM International Conference on Image and Video Retrieval*, CIVR '10, pages 189–196, New York, NY, USA, 2010. ACM.
16. Nicola Bicocchi, Gabriella Castelli, Marco Mamei, Alberto Rosi, and Franco Zambonelli. Supporting location-aware services for mobile users with the whereabouts diary. In *Proceedings of the 1st international conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications*, MOBILWARE '08, pages 6:1–6:6, ICST, Brussels, Belgium, Belgium, 2007. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
17. Lukasz Jedrzejczyk, Blaine A. Price, Arosha K. Bandara, and Bashar Nuseibeh. On the impact of real-time feedback on users' behaviour in mobile location-sharing applications. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 14:1–14:12, New York, NY, USA, 2010. ACM.
18. Drew Fisher, Leah Dorner, and David Wagner. Short paper: location privacy: user behavior in the field. In *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices*, SPSM '12, pages 51–56, New York, NY, USA, 2012. ACM.

19. Mary Madden, Amanda Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, Aaron Smith, and Meredith Beaton. Teens, social media, and privacy. In *http://www.pewinternet.org//˜media//Files/Reports/2013/PIP_TeensSocialMediaandPrivacy.pdf*, May 2013.
20. Google Developers. Kml documentation introduction. In *https://developers.google.com/kml/documentation*.