Hindawi Publishing Corporation
Advances in Human-Computer Interaction
Volume 2014, Article ID 678165, 23 pages
http://dx.doi.org/10.1155/2014/678165

Research Article

Users Behavior in Location-Aware Services: Digital Natives versus Digital Immigrants

Marco Furini

Dipartimento di Comunicazione ed Economia, Università di Modena e Reggio Emilia, Viale Allegri 9, 42121 Reggio Emilia, Italy

Correspondence should be addressed to Marco Furini; marco.furini@unimore.it

Received 24 October 2013; Revised 29 January 2014; Accepted 5 February 2014; Published 19 March 2014

Academic Editor: Zhiwen Yu

Location-aware services may expose users to privacy risks as they usually attach user's location to the generated contents. Different studies have focused on privacy in location-aware services, but the results are often conflicting. Our hypothesis is that users are not fully aware of the features of the location-aware scenario and this lack of knowledge affects the results. Hence, in this paper we present a different approach: the analysis is conducted on two different groups of users (digital natives and digital immigrants) and is divided into two steps: (i) understanding users' knowledge of a location-aware scenario and (ii) investigating users' opinion toward location-aware services after showing them an example of an effective location-aware service able to extract personal and sensitive information from contents publicly available in social media platforms. The analysis reveals that there is relation between users' knowledge and users' concerns toward privacy in location-aware services and also reveals that digital natives are more interested in the location-aware scenario than digital immigrants. The analysis also discloses that users' concerns toward these services may be ameliorated if these services ask for users' authorization and provide benefits to users. Other interesting findings allow us to draw guidelines that might be helpful in developing effective location-aware services.

1. Introduction

Location-aware services are very popular among smartphone owners as they allow users to receive customized services and/or resources like weather updates, tourist information when walking in a certain area of a visited city, digital coupons from restaurants in the nearby, and detailed traffic information of the area where they are; furthermore, these services allow users to perform several different and novel activities like social rendezvous, local friend recommendations for dining and shopping, collaborative networked games, and altruistic services [1–4]. Examples of applications that provide location-aware services are, just to name a few, Foursquare, Facebook Places, Twitter, Yelp, Instagram, Runkeeper, Endomondo, and Google Maps.

The user's location is usually available through voluntary user's check-in in applications like Foursquare and Facebook Places or is produced by the applications (through technologies like GPS, cellphone network triangulation, RFID, and IP address geolocation). Regardless of the way this information is generated, when users post/share contents through location-aware applications, the produced contents are usually coupled with the user's geographical location and with a lot of other information like device type, capture time, and OS language. By combining these pieces of information with the user's location and with the popular functionalities of social networks and of social media, the applications behind these services are likely to be very important for the next-generation mobile computing [5].

If on the one side the access to the user's location is mandatory to provide a customized service, there are numerous real-world examples where users' locations are collected for other purposes. For instance, third-party analysis may reveal users' habits (e.g., an adversary might be able to observe multiple user's presence at the same place like hospital, liquor store, pub, and hotel) and sensitive information (e.g., an adversary may infer that a user is not at a certain place at a given time or may understand which data a user finds interesting), may facilitate criminal activities (e.g., an adversary may know what itinerary a user does during the day), and may gather legal evidence [1]. With no doubt, a deep study of data available and accessible in social media

platforms can reveal a wealth of information about a specific user and this may lead to personal privacy risks [6].

In the literature, there has been a significant amount of research on the privacy issue in mobile applications and much of this research has been focused on location privacy. The results are often conflicting and do not allow having a clear picture of the location-aware scenario: some studies say privacy concerns may compromise the success of location-aware services [7], others say users are not concerned about privacy and therefore are willing to enter the scenario [8], and others say users need advance privacy settings to alleviate privacy concerns [9, 10]. In our opinion, this lack of clarity is due to the infancy stage of the location-aware scenario and to the methodology used to investigate users' attitudes and opinions toward privacy in a location-aware scenario.

Convinced that, to build an effective location-aware scenario, it is necessary to clearly understand users' attitudes toward privacy, this paper presents a different approach to investigate privacy concerns toward location-aware services. Indeed, since the location-aware scenario is in its infancy stage, users may not be fully aware of its features. This lack of knowledge may affect the results of the investigation, and therefore, we conduct our analysis in two separate steps: (i) the initial step aims at understanding what users know about the location-aware scenario; (ii) the second step aims at investigating users' opinion toward location-aware services, but the investigation is done after showing users examples of location-aware services able to extract personal and sensitive information from contents publicly available in social media platforms. In this way, the analysis will reveal if there is a relation between users' knowledge and users' concerns toward location-aware services. Indeed, our hypothesis is that, without splitting the analysis, it would be difficult to say if a lack of concern is due to a lack of knowledge or not. Moreover, we think it is important to highlight the difference between digital natives and immigrants as digital natives are usually considered early adopters of new technologies and services and therefore their current behavior is a good indicator of what will happen in the near future. Therefore, our study analyzes two different categories of users: digital natives and digital immigrants [11]. The former group is composed of users who were born during or after the general introduction of digital technologies, whereas the latter group is composed of individuals who were born before the existence of digital technology and adopted it to some extent later in life. To the best of our knowledge, there are no previous studies that consider the relation between users' knowledge and users' concerns toward location-aware services and analyze/compare digital natives and digital immigrants concerns toward privacy in a location-aware scenario.

Our hypothesis is confirmed by the obtained results: the first step of the investigation shows that users are not really concerned about privacy and shows that users ignore many of the features of location-aware services, but the second step of the investigation shows that privacy concerns arise after users are faced with a location-aware application able to extract personal information from contents publicly available in social media platforms. In particular, the analysis reveals that there is relation between users' knowledge and users' concerns toward privacy in location-aware services and also reveals that digital natives are more interested in the location-aware scenario than digital immigrants. The analysis also reveals that users' concerns toward these services may be ameliorated if these services ask for users' authorization and provide benefits to users (i.e., users are willing to share their personal location as long as there are personal benefits). Based on the obtained results, we provide guidelines that might be helpful to develop effective location-aware services.

The remainder of the paper is organized as follows: Section 2 presents an overview of studies that focused on the privacy aspect of location-aware services; Section 3 describes details of the first step of the investigation, whereas Section 4 presents details of the second step of the investigation. Guidelines to develop effective location-aware services are drawn in Section 5 and conclusions are presented in Section 6.

2. Related Work

In the following, we review studies related to privacy in location-aware applications by grouping them into three categories: (i) management of privacy settings, (ii) disclosure of personal geographic location, and (iii) users' concerns about the sharing of personal geographic location.

2.1. Management of Privacy Settings. Users have difficulties in expressing and setting their privacy preferences; they manage privacy policies only marginally; they are not very good at understanding the future value of keeping personal information private; they consider privacy settings a time-consuming process; they do not really care about privacy settings until their privacy is violated. These are some of the findings that different studies highlighted (e.g., [9, 10, 12, 13] just to name a few).

In the attempt to help users in taking privacy decisions, some studies proposed to design privacy management systems able to handle privacy settings in an easy and effective way. For instance, Jedrzejczyk et al. [12] designed a location-sharing mobile application, called Buddy Tracker, which provides several options for managing privacy: accountability (it provides a feedback when a personal location is checked by someone else), awareness (users are informed with ad hoc warnings that are displayed on the mobile device about how and who access information about their position), and visibility (users can make themselves invisible for a period of time). Results obtained from an experimental evaluation showed that the proposed system may help protecting users' privacy, as it makes users more responsible.

Other studies investigated the possibility of automatically set privacy options according to the preferences taken by users in the past. The results are conflicting: some studies say it is possible (e.g., [10, 14]); others say a priori configuration settings of applications that disclose private information will not work (e.g., [15, 16]).

2.2. Disclosure of Personal Geographic Location. In the literature, different studies agreed that users do not disclose

their personal position to anyone, nor they share it with any application.

Consolvo et al. [6] showed that the decision to disclose personal geographic locations depends on many different factors: *who* is the requester, *why* the requester wants to know the location, and *what detail* would be the most useful to the requester. Other factors include the relationship with the applicant (users are more willing to share information with significant others/spouses (93%), friends (85%), and family (83%)), the place where the user is located (it is more likely that users share their location while at home than at work), the activity that is taking place (96% share personal location if they are doing household chores, 84% if they are exercising, 81% if they are talking on the phone, and 63% when studying), and the mood (82% disclose personal location if they are depressed, 77% if they are happy or relaxed, 72% if they are stressed, and 64% if sad).

Burghardt et al. [17] obtained similar results while asking which information users would like to share with others. By designing and implementing a fully operational geotagging service and by letting participants use this application in their daily lives, the obtained results showed that, among all the users who downloaded a location-aware mobile application, 95% shared their location with friends, 92% with classmate, 91% with parents, and 86% with anybody.

Fisher et al. [10] investigated if users are willing to share their location with any application requesting it, or if users filter applications somehow. Results obtained from investigating the behavior of users when dealing with the 25 applications installed on most phones showed that users grant access to applications where the location information is critical for the application functioning but deny access when it is less clear what benefits location-sharing can bring to them. For instance, around 60% of users grant access to Twitter, more than 60% allow Instagram to access to their location, around 70% grant access to Google, more than 80% to weather applications, around 90% for Yelp, and the percentage increases to 97% for maps applications.

Ahern et al. [18] analyzed the behavior of users when sharing photos with smartphone devices. By allowing users to use ZoneTag, a mobile application that automatically adds location data to a photo before uploading it to the Flickr website, authors investigated how users check and modify privacy settings. Results showed that only 2% of the users blocked the sharing of personal location. Therefore, it seems that users are not concerned in showing their personal position when shooting photos. Authors also investigated if there is any relationship between photo content and privacy. Results obtained showed that users with family and children seemed particularly concerned about the publication of their photos. Similarly, they were concerned about children safety and house privacy. This reflects that, when photos are about users or personal places, users tend to be more careful.

Kelley et al. [9] investigated whether users are comfortable in disclosing their location with advertisers. The study highlighted that place and amount of messages received are factors that affect the decision of sharing personal location with advertisers; also, users are more willing to share their location on weekdays from 9 to 17 (probably while they are at work or at school). In general, the study showed that users' privacy concerns may hinder the adoption of systems based on location-aware technologies and that advance privacy settings may help alleviate some of these concerns.

2.3. Concerns of Users with respect to the Sharing of Personal Geographic Information. What are the users' concerns (if any) when using applications that access to location-aware technologies? Ahern et al. [18] investigated what users would feel if their personal position would be disclosed to third parties. The majority of respondents expressed little or no concerns at all. A different finding has been obtained by Barkus [7]: users are initially concerned about their privacy, but their level of concern diminishes when they are actually using geolocation services. Indeed, users find these services less intimidating after using them.

Chin et al. [8] analyzed users' privacy concerns when using smartphones. Results showed that, in general, users are more concerned and anxious when using smartphones than personal computers. In particular, privacy concerns arise when users deal with financial applications and when entering sensitive personal data. When asked about their location, all participants except one were in favor to disclose their location: this indicates that the benefits provided by geosocial applications exceeded their apprehensions.

According to the studies related to location privacy, users behavior is not clear. Roughly speaking, some say users are concerned about privacy when using location-aware applications and some say they are not. In our opinion, this is mainly due to the used methodology that does not consider that users may be not fully aware of the features of the location-aware scenario as the scenario is in its infancy stage. Indeed, the lack of knowledge may affect the results. For this reason, in the following, we consider a different approach: instead of investing users' concerns toward privacy in location-aware services in a single step, we conduct our analysis in two separate steps and we analyze two categories of users: digital natives and digital immigrants. The analysis in two steps is important as it will reveal if there is a relation between what users know about the features of a location-aware scenario and what users think about privacy when using location-aware services. The analysis of the two groups of users is important because digital natives are considered early adopters of new technologies and services and therefore they are the most exposed to the privacy risks, not to mention that the future location-aware scenario will be mainly composed of digital natives.

As mentioned, to the best of our knowledge there are no previous studies that consider the relation between users' knowledge and users' concerns toward location-aware services and analyze/compare digital natives and digital immigrants concerns toward privacy in a location-aware scenario.

3. Location-Aware Services: Technological Equipment and Users' Knowledge

To develop effective location-aware services, it is important to know users' opinions toward privacy in location-aware services. The previous section showed that some studies say

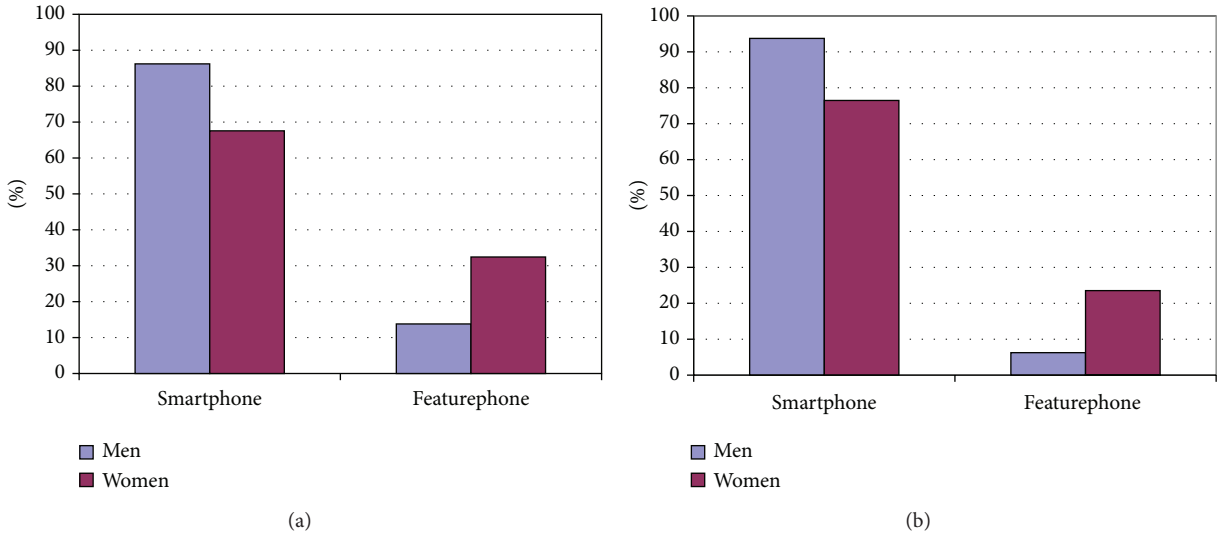


Figure 1: Technological equipment: smartphone penetration among digital natives (a) and digital immigrants (b).

users are concerned about privacy, while other studies say they are not. In our opinion, these conflicting results are due to the infancy stage of the location-aware scenario and to the methodology used to investigate users' attitudes and opinions toward privacy when using location-aware services. Indeed, our hypothesis is that the lack of knowledge of the location-aware scenario features may affect the results of the investigation. Therefore, to have a clear picture of what users think about privacy in location-aware services, we think it is necessary to split the investigation into two parts: (i) understand what users know about the location-aware scenario and (ii) understand users' opinions toward location-aware services. Note that, to reveal if there is a relation between users' knowledge and users' concerns toward location-aware services, the second part of the investigation is done after showing users examples of location-aware services able to extract personal and sensitive information from contents publicly available in social media platforms. Moreover, we think it is important to highlight the difference between digital natives and immigrants as digital natives are usually considered early adopters of new technologies and services and therefore their current behavior is a good indicator of what will happen in the near future. It is worth recalling here that, since there is not a clear distinction between digital natives (DNs) and digital immigrants (DIs) (some say 1980 is the year that separates the two generations and others say 1990), in this paper we consider users younger than 25 years old as belonging to the digital native group and the others belonging to the digital immigrant group.

In the following, through a real-world study, we investigate what users know about the location-aware scenario, whereas the second part of the investigation will be presented in the next section.

Through different technological platforms, we asked users to voluntarily participate in the real-world study. It is worth noting that, even though voluntary response samples are usually biased, in our study the voluntary participation does not affect the results. Indeed, since we are interested in users who daily use technological devices and applications (i.e., users who consider mobile technologies and applications as commodities in their daily life), we used different technological platforms to get in touch with these users. Therefore, all the users who voluntarily participated in the real-world study are users who daily use technological devices and applications. Forcing the sample to include other users would have produced a sample to which we were not interested.

We have been contacted by 66 DN users (54% women and 46% men), and by 66 DI users (also in this case, 54% women and 46% men). Within the DN group, 76% are students and 21% are employees. Within the DI group, 57% are employees, 34% are students, and 5% are entrepreneurs. Before presenting the results, it is worth mentioning that the sociodemographic aspect was investigated at the end of the questionnaire because personal questions may cause respondents to answer defensively the rest of the questionnaire, thus reducing the value of the results and therefore affecting the overall investigation. Conversely, by putting the sociodemographic investigation at the end of the questionnaire, respondents feel the questionnaire anonymous and therefore results should better reflect the real-world scenario.

3.1. Technological Equipment and Users' Habits. The investigation aims at understanding what users know about the mobile device and the location-aware technologies and what are the habits of the participants in the mobile scenario (data subscription plan, download of mobile applications, and usage of geolocation services).

Figure 1 reports the percentage of users who own a smartphone or a featurephone. Results show that smartphone penetration is very high in both groups. In particular, it is higher among DIs (on average 77% among DNs and 85% among DIs), probably due to higher cost of these cellphones. The analysis also reveals that the smartphone penetration is

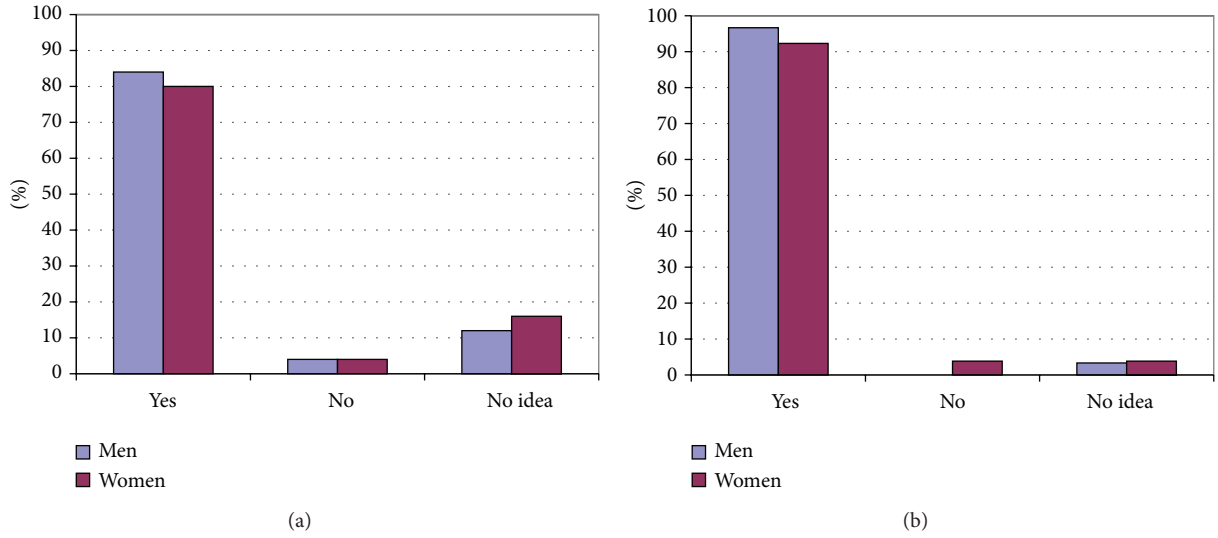


Figure 2: Technological equipment: GPS-availability within smartphones. DN (a) and DI (b).

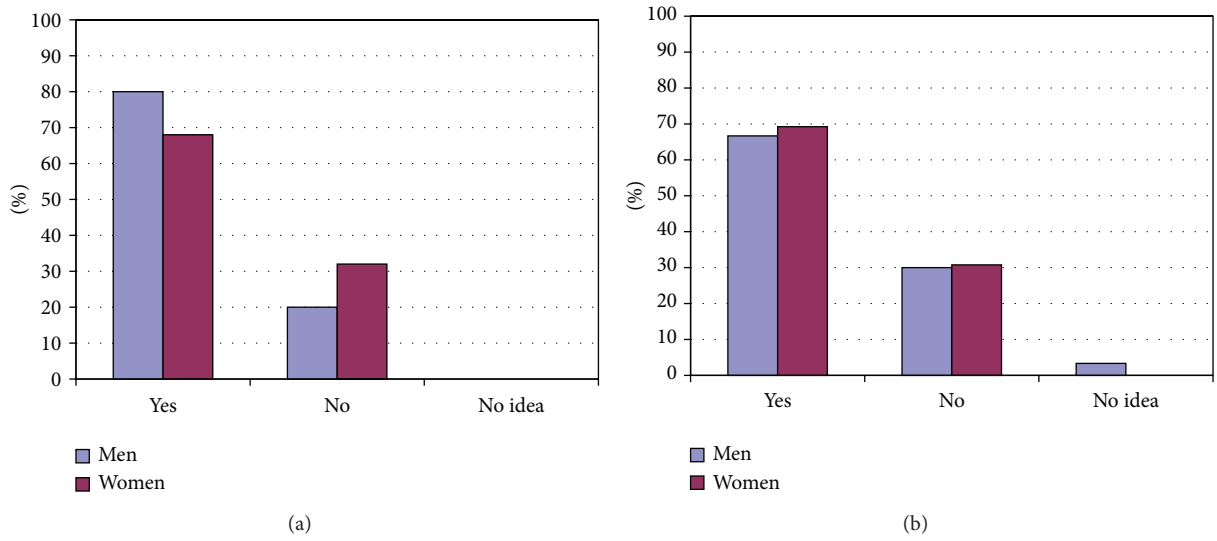


Figure 3: Users who use location-aware applications: DN (a) versus DI (b).

higher among men than among women (86% versus 68% among DNs and 94% versus 76% among DIs).

The high smartphone penetration facilitates the access to the Internet: results obtained by asking participants if their device is connected to the Internet show that, among smartphone owners, 94% of DNs and 91% of DIs are always connected to the Internet through flat-rate data plans. Therefore, if one thought that the cost of a smartphone and the cost of the Internet connection were an obstacle (especially for DNs) for the usage of location-aware services, results obtained show that they are not.

To investigate the knowledge users have about their smartphone, we asked participants whether their device is equipped with GPS technology or not. Results presented in Figure 2 show that the percentage of devices with GPS is above 80% within DN members and above 90% within DI members. The analysis reveals that DNs are less informed than DIs about the technologies available in their device: the percentage of users who ignore the GPS availability within their device is 12–16% within the DN group and 3-4% within the DI group.

To understand the relationship between users and mobile applications, we asked participants whether they have downloaded at least one application over their smartphone and if they use applications that exploit location-aware technologies. The investigation reveals that 100% of DIs claim to have downloaded, on its own initiative, at least one application over their smartphones and also reveals that, within the DN group, 8% of women say they never downloaded an application over their smartphone.

Figure 3 shows results obtained while asking users if they use location-aware applications: a large majority of

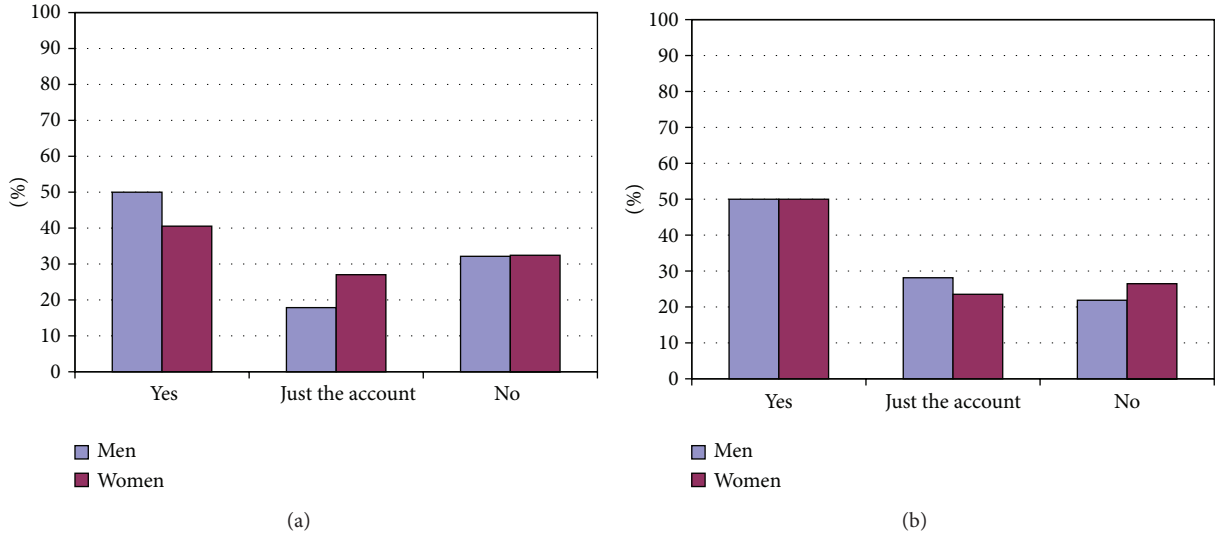


Figure 4: Twitter presence: DN (a) versus DI (b).

participants (on average, 74% among DNs and 68% among DIs) use location-aware applications, whereas only 3% of men in the DI group have no idea. The entire group of DNs are aware if they use a location-aware application or not, and this may contrast the results obtained when investigating the GPS availability within smartphone. This reveals that DNs are not interested in the technology itself but are more focused on the results obtained by applying that specific technology (e.g., they do not know if their device is equipped with GPS, but they know if they use a location-aware application, or, with a different perspective, they know what a location-aware application is, but they do not know, or do not care, what technologies are necessary to run the application).

3.2. Basic Knowledge of Location-Aware Services. The investigation aims at understanding how users interact with location-aware applications that share user-generated contents in social media platforms. In particular, we focus on two very popular mobile applications: Twitter (the microblogging social platform that allows publishing messages up to 140 characters) and Instagram (the social platform that allows users to apply filter effects and to share their photos). These applications allow users to share their contents with other users in an easy way and they also exploit location-aware technologies as they attach to user-generated contents the user's location (if available).

Figure 4 reports the Twitter presence grouped in three categories: users who do not have an account, users who have an account but never use the application, and users who use the microblogging platform. Results show that there is no significant difference between DNs and DIs: in both groups half of the participants use Twitter. Looking at DNs, Twitter is more popular among men than among women.

Figure 5 reports the Instagram presence grouped in three categories: users who do not have an account, users who have an account but never use the application, and users who use the photo sharing platform. Results show that the photo-sharing platform is more popular among DNs than among DIs (60% versus 53% among men and 72% versus 45% among women).

The comparison between Twitter and Instagram reveals that, within the DN group, users prefer sharing photos than tweets as Instagram is more popular than Twitter: 60% versus 50% for men and 72% versus 41% among women.

Social media platforms like Twitter and Instagram allow users to customize their profile type in two possible ways: public or private. In both platforms the default setting is public (contents are visible to anyone, regardless they have an account or not) and therefore users who want to restrict the access only to approved friends have to change the profile settings. To investigate the way users share their contents, we asked participants about the type of profile they have.

Figure 6 shows the profile type of the Twitter users. Among DNs, the percentage of users who ignore their profile type is considerable: 27% among men and 40% among women. The remaining DNs slightly prefer the public profile. The situation is different when analyzing the DI group: the majority of men prefer the public profile (48%), whereas the majority of women prefer the private profile (48%). The percentage of users who have no idea about their profile is similar: 16% (men) and 20% (women).

Figure 7 shows the profile type of the Instagram users. Again, among DNs, the percentage of users who have no idea about their profile type is considerable: 35% among men and 29% among women. The remaining DNs slightly prefer the public profile (35% of men and 52% of women). Within the DI group, the percentage of users who ignore their profile type is considerable for women (47%) and for men (24%). The majority of men prefer the public profile (48%).

The comparison between Twitter and Instagram reveals that DIs are less informed about Instagram than about Twitter (probably due to the fact that Instagram is a recent application) and also reveals that around one-third of DNs ignore the characteristics of their profile. Since a considerable

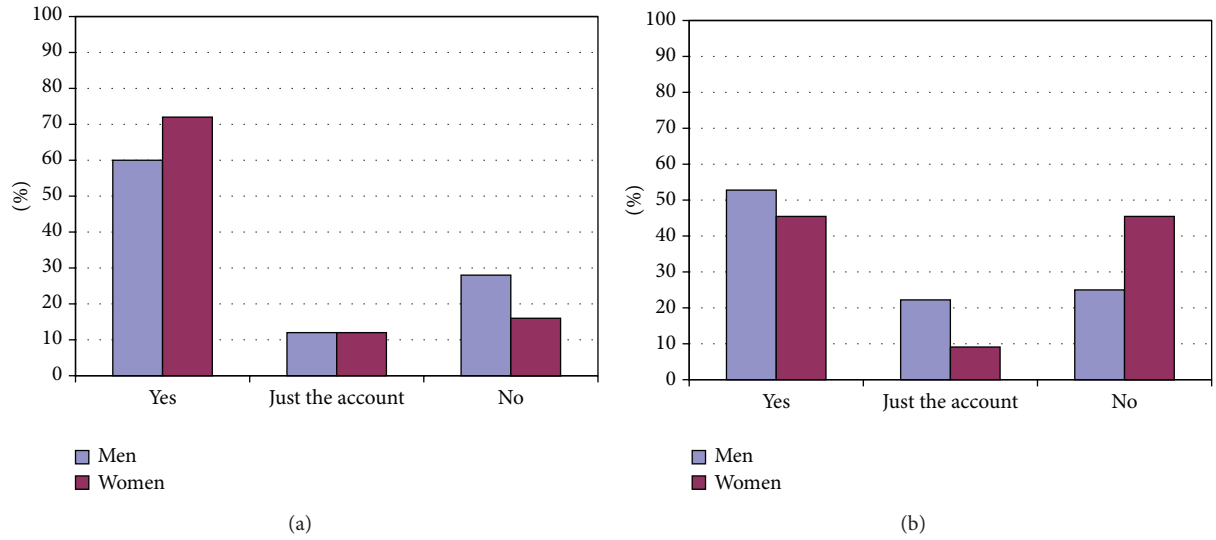


Figure 5: Instagram presence: DN (a) versus DI (b).

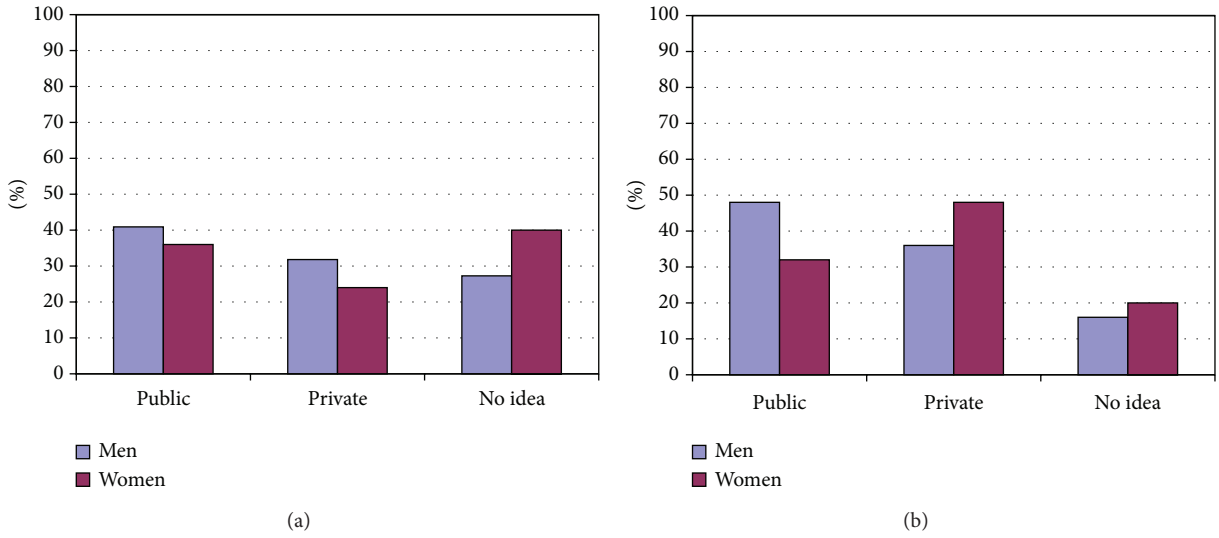


Figure 6: Type of personal profile over Twitter: DN (a) versus DI (b).

percentage of users ignore their profile type it is likely that these users ignore who can access their user-generated contents. Moreover, since the percentage of users who use the public profile is quite high, it is reasonable to assume that most of user-generated contents (either tweets or photos) are publicly available on the two platforms.

Figure 8 reports the percentage of users who use the geolocation technology within Twitter: a considerable number of DNs ignore this feature (32% of men and 56% of women) and also within the DI group the geolocation feature is not clear to everybody: 24% of men and 20% of women have no idea if they use this feature or not. It is to highlight that 44% of DI men use this feature.

Figure 9 reports the percentage of users who use the geolocation feature within the Instagram platform. Again, a large number of DNs have no idea if they use this feature or not (60% of men and 41% of women). Similarly, a considerable number of DI members ignore this feature (33% of men and 41% of women). It is interesting to note that 62% of DI men use this feature.

The analysis reveals that a significant number of users (more among DNs than among DIs) ignore the geolocation feature. Likely, users associate location-aware applications with maps, weather updates, news information, and so forth, but tend to forget that some applications asked for permission to access users location when installed. For this reason, when asked about the usage of location-aware applications they replied with either yes or no, but when asked if they use geolocation feature within Twitter or Instagram, a large percentage of them have no idea about it.

Other interesting findings are that users prefer using the geolocation feature when sharing photos, and that DI men love using this feature either when sharing tweets or photos.

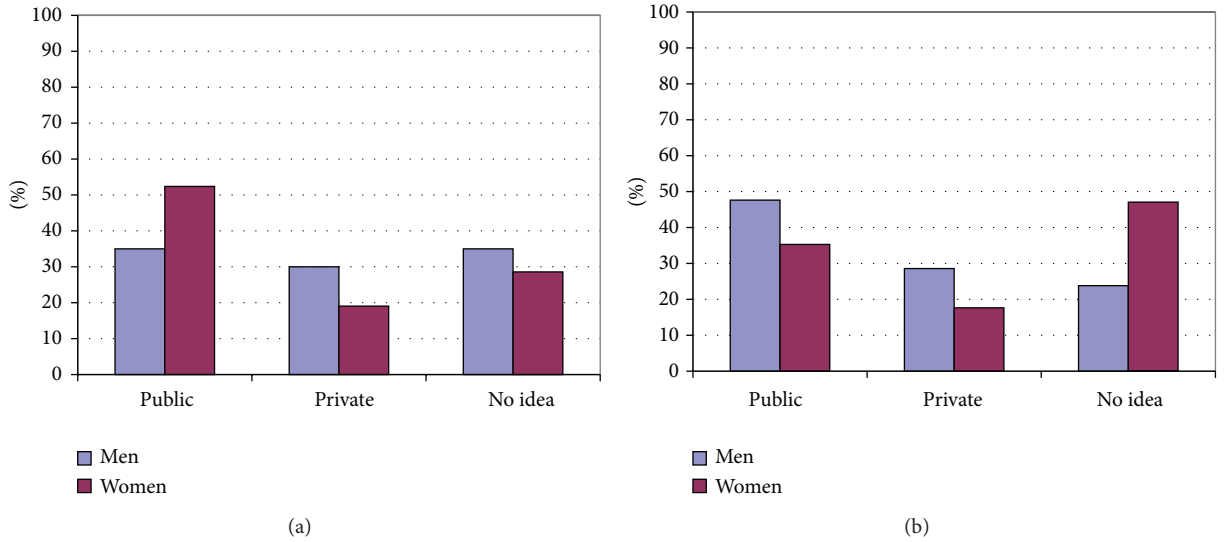


Figure 7: Type of personal profile over Instagram: DN (a) versus DI (b).

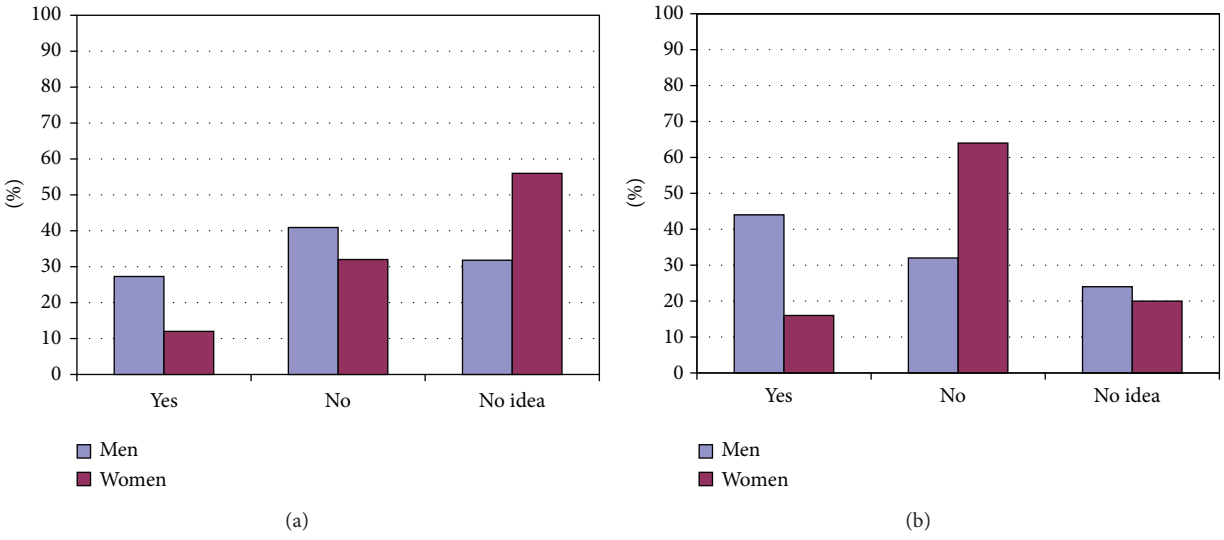


Figure 8: Usage of the geolocation feature within Twitter: DN (a) versus DI (b).

The reasons to use the geolocation technology are reported in Figure 10: among DNs, men use this feature "To let others find my photos" (44%), whereas women use this feature to "let others know where I am" (60%). Among DIs, women use this feature "to let others find my photos" (64%), whereas men use this feature for different reasons, either personal ("To remind me where I've been" or "To let others know where I am") or altruistic ("To let others find my photos").

The large number of users who ignore how user-generated contents are shared in social media platforms likely causes these contents to contain user's location and to be publicly accessible in social media platforms. As a consequence, a privacy risk may arise, but what do users think about privacy? Did they change privacy settings at least once after the registration to the Twitter/Instagram platforms?

Figure 11 shows that the majority of DNs (50% among men and 60% among women) and a considerable number of DIs (more than 40%) do not remember changing their privacy settings in the Twitter platform. The scenario is similar in the Instagram platform: Figure 12 shows that the majority of DN members (75% among men and 41% among women) and a considerable number of DIs (38% among men and 53% among women) have no idea about changing their privacy settings.

The obtained results show that users are not concerned about privacy. Indeed, although DIs are more informed than DNs, in general users do not have idea about privacy settings or personal profile type. As a consequence, it is likely that most of the user-generated contents are publicly available and contain user's geographical location.

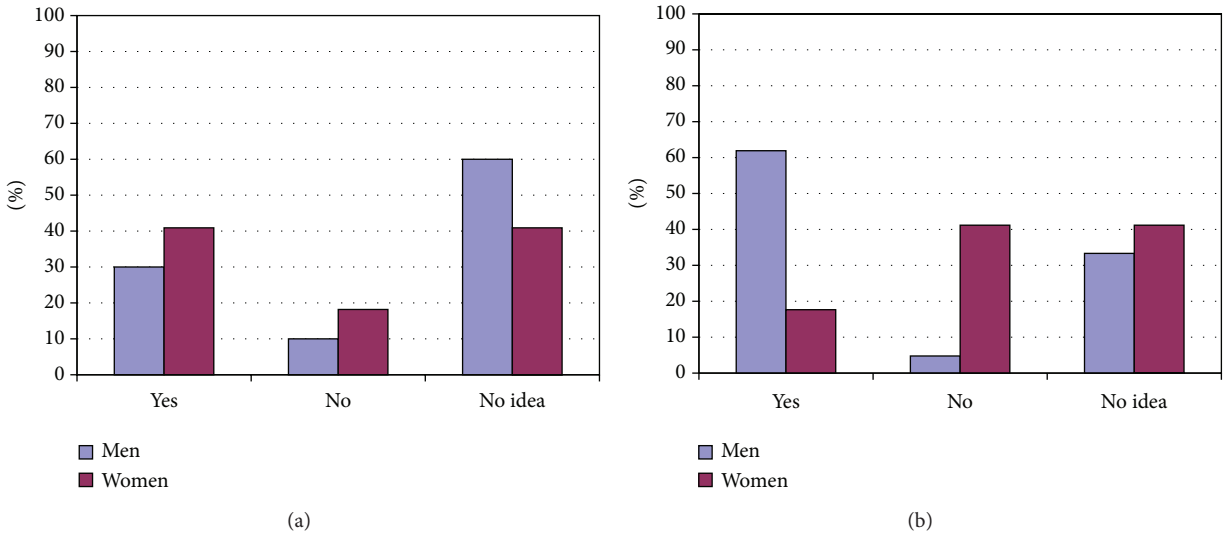


Figure 9: Usage of the geolocation feature within Instagram: DN (a) versus DI (b).

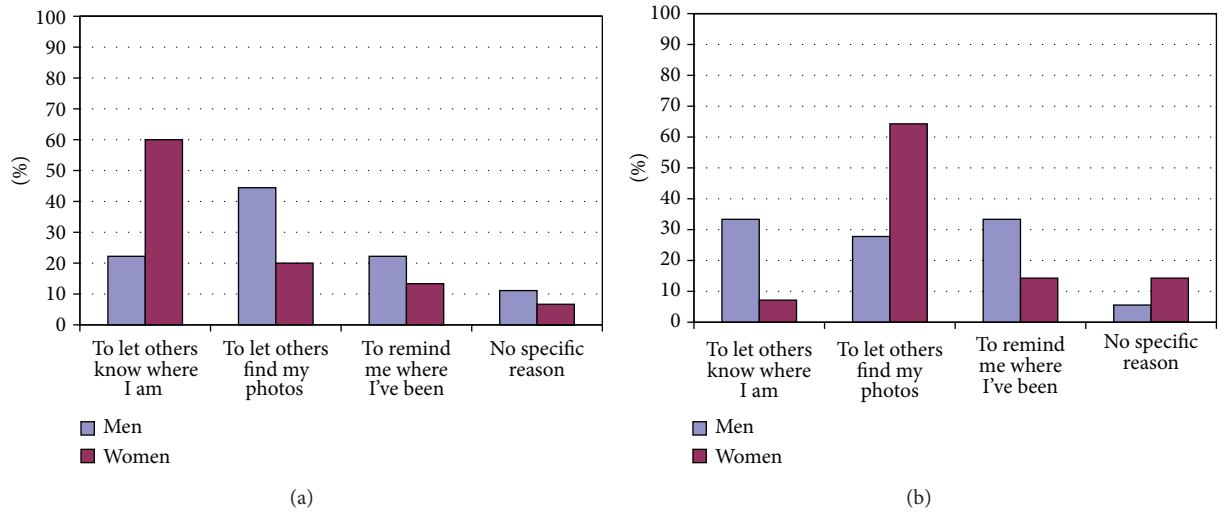


Figure 10: Reasons to use the geolocation feature: DN (a) versus DI (b).

3.3. Summary of Results and Main Findings. The first part of the study investigated what users know or ignore about the features of the device they own and the features of the applications they download and use. In summary, the analysis revealed the following.

(i) Technological knowledge: the majority of users own advanced cellphones, download and use mobile applications, and are always connected to the Internet through flat-rate data plans. If one thought that the cost of smartphone or the cost of Internet mobile data traffic were an obstacle for the usage of location-aware services, the results obtained show that they are not; the analysis revealed that DNs are less informed than DIs about the features of their device. This confirms that DN and DI are different learners: as reported in [19], DN members have fun with technology, but they usually do not read manuals, whereas DI members are accustomed to and prefer manuals as they like a logical and linear process of discovery. The obtained results show that DNs are not interested in the technology itself (e.g., they have no idea whether GPS technology is embedded into their smartphone or not) but are more excited about the application of the technology (e.g., they know whether they use location-aware applications or not). Indeed, DNs are more informed than DIs about the mobile application features but are less informed than DIs about the technology used to achieve these features.

(ii) Social media presence: around half of DNs and of DIs use Twitter; Instagram is used by more than 60% of DNs and around 50% of DIs. The photo-sharing application is more used than the microblogging platform both within the DN group and within the DI group.

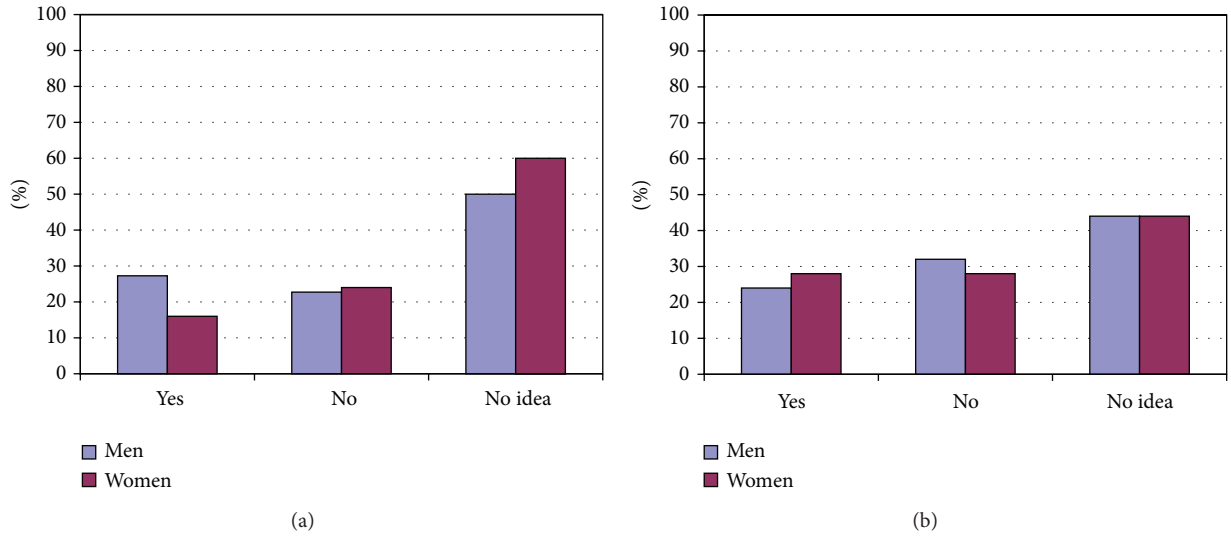


Figure 11: Changes to privacy settings on Twitter. DN (a) and DI (b).

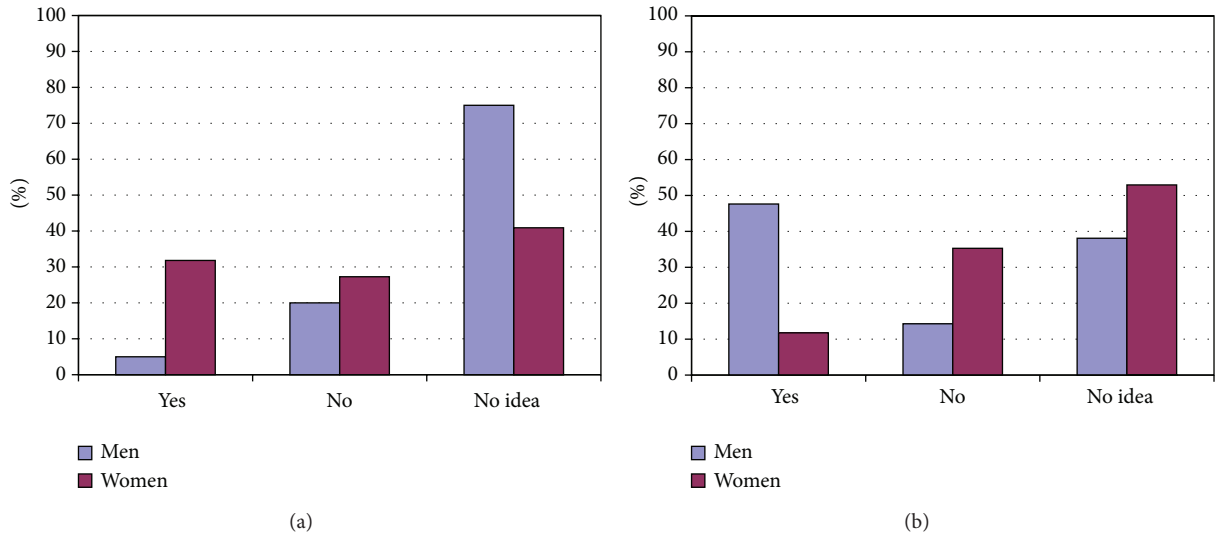


Figure 12: Changes to privacy settings on Instagram. DN (a) and DI (b).

(iii) Privacy concerns: users are not interested in privacy. The percentage of users who ignore their profile type, who ignore the usage of the geolocation feature, and who ignore if they changed their privacy settings is very high. The main difference between DNs and DIs is that the percentage of users who ignore these characteristics is higher among DNs than among DIs. Once again, this confirms that DNs have fun with technology, but they are not aware/interested in the possible side effects of using technology. Another interesting result is that a considerable number of users set their profile type as public, use geolocation feature (DI men love using this feature when sharing tweets and photos, and, in general, many users use this feature when sharing photos), and did not change their privacy settings. As a consequence, the majority of user-generated contents are probably available and accessible on the two platforms.

The high percentage of users who ignore their profile type, who ignore the usage of the geolocation feature, and who ignore if they changed their privacy settings has two possible reasons: (i) users are not interested in privacy, or (ii) the location-aware scenario is in its infancy stage and therefore is an obscure scenario for many users. In the following, to better understand users' opinions toward privacy when using location-aware services, we show them examples of personal and sensitive data extracted from contents publicly available in social media platforms and then we will ask users for their opinions.

4. Location-Aware Services: Opinions and Preferences

The second part of the investigation aims at understanding users' opinions toward privacy when using location-aware services. However, since the location-aware scenario is in its infancy stage, users may not be fully aware of the power of location-aware services and this lack of knowledge would likely affect the obtained results. For this reason, before investigating users' opinions toward such services, we show them examples of personal and sensitive information that can be retrieved by a simple location-aware application that accesses to user-generated contents available in public social media platforms.

4.1. An Application Prototype to Extract Sensitive Information from Social Media Platforms. To show that anyone (neighbor, friends, etc.) can extract personal and sensitive information from contents publicly available in social media platforms, we developed a prototype application that exploits social media APIs to access public geotagged contents, and combines and filters the retrieved contents to extract personal and sensitive information. It is worth noting that in the prototype we focus on Twitter and on Instagram, but it is possible to expand the prototype with additional social media platforms if the corresponding APIs are available. There is no need to install the application in the users' mobile device and there is no need to log-in to social media platforms to access to user-generated contents. Since details of the prototype application go beyond the scope of this paper, in the following we present examples that show the personal information that is possible to obtain by accessing to user-generated contents (e.g., tweets or photos) and to the associated information (e.g., geolocation data, creation time, author name, username, device type, preferred language, etc.). To this aim, we randomly selected ten users among the ones located in the nearby of our Department. As we show, the access to a single tweet is sufficient to discover several personal information, while to obtain user's habits it is sufficient to access a sequence of the most recent user's tweets (i.e., from our experiments we realized that the 25 most recent user's tweets were sufficient to find habits and personal information like home/school/work address).

Figure 13 shows the personal information that can be obtained by accessing the metadata of a single tweet (we have obscured sensitive data for privacy reasons): username, name, surname, current geographical position, language, personal photo, city, personal website address, and number of Twitter followers and following. It is worth recalling here that all these pieces of information are publicly available (they are associated with the user's generated contents).

Table 1 summarizes the personal information that was possible to retrieve, for the ten monitored users, by simply browsing data publicly available in social media platforms. For every user it was possible to know the device type and the preferred language, for nine out of ten it was possible to know the sex, and for eight out of ten we know the home/school/work address.

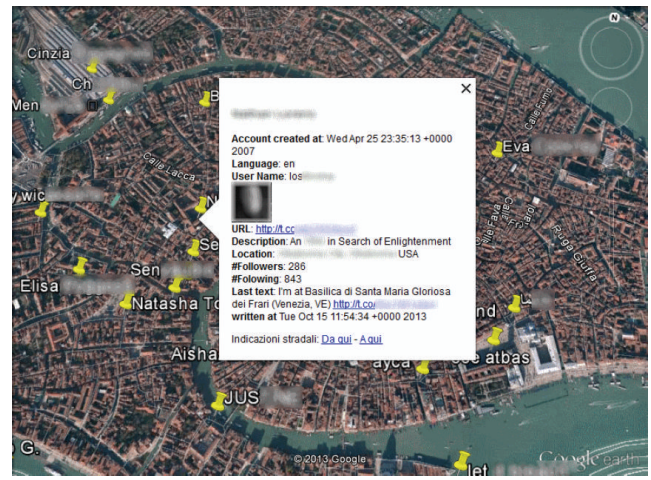


Figure 13: Personal and sensitive information available in the metadata of a single tweet.

The home/school/work address is obtained by looking at the locations where the most recent contents were produced: for most of the monitored users, we noticed two main clusters, as shown in Figure 14, one composed of contents generated in the evening and early in the morning and the other composed of contents generated during the morning/day. Likely, the location of one cluster is the home address, and the location of the other is the work/school address (only user number 3 and user number 4 did not generate clusters and by considering that these users were the only ones whose preferred language was not Italian; we infer these users were tourists).

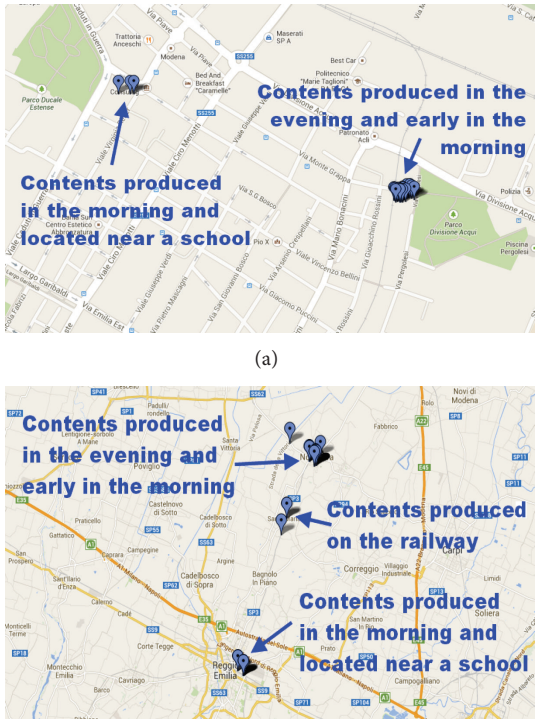
Furthermore, by looking at the recent history of user's produced contents it is possible to discover personal habits (e.g., the route to work) or specific personal information (e.g., the cellphone operator or the preferred TV show), as shown in Table 2. For instance, for user number 1 we know several details, whereas for users number 3 and number 4 (the users on vacation) we were not able to find habits by looking at the 25 most recent tweets.

These are just some examples of personal information that third parties can extract by simply accessing user contents available in social media platforms. Needless to say, it is possible to have a very detailed profile of every user by performing a more detailed investigation (e.g., by looking at more tweets/photos or by aggregating these data with Google street view or with other social media platforms). These data can be very useful for third parties like employers (what is the employee doing in a bar while he should be home sick?), teammates (why is the partner in a hotel instead of being at work?), insurance companies (why the insured person who claims to be in good health often attends doctors or hospitals?), bad guys (that person frequents the park every day at a certain time), thieves (the house of that family is blank because they are on holiday on the other side of the world), marketing analysts (that person attends always that kind of supermarket or that particular store), and so forth.

Table 1: User's personal information retrieved by aggregating the 20 most recent tweets/photos.

User number	Language	Name	Sex	Home address	Work/school address	Work/school type	Device type
1	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2	Yes	No	Yes	Yes	Yes	Yes	Yes
3	Yes	Yes	Yes	Yes*	No	No	Yes
4	Yes	Yes	Yes	Yes*	No	No	Yes
5	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6	Yes	No	No	Yes	Yes	Yes	Yes
7	Yes	Yes	Yes	Yes	Yes	Yes	Yes
8	Yes	Yes	Yes	Yes	Yes	Yes	Yes
9	Yes	Yes	Yes	Yes	Yes	Yes	Yes
10	Yes	Yes	Yes	Yes	Yes	Yes	Yes

*Just the city and not the home address.



(a)

(b)

Figure 14: Examples of personal information inferred by combining location and content production time of the 25 most recent contents produced by a user.

4.2. Users Opinions: Reactions, Willing to Be Contacted, and Definitions. The prototype application showed that it is possible for third parties to access, in an anonymous way, personal and sensitive data. Since in the near future, many new location-aware services will likely be available, we ask participants for their opinions toward third-party services.

The first question investigates what would be the reactions if third parties would access and use user's location to extract personal and sensitive data from contents publicly available. Figure 15 reports results obtained when considering users who claim to use location-aware services and when considering users who claim not to use these services. Results obtained while analyzing the DNs behavior (Figures 15(a) and 15(b)) show that users who claim to not use location-aware applications are more concerned and worried about these services: more "Angry," "Discomfort," and "negative consequences" answers than the ones obtained by users who claim to use location-aware services. A similar behavior can be observed in Figures 15(c) and 15(d) when analyzing DIs. In general, results show that DNs are more worried and concerned about these services (see, DN men versus DI men, Figure 15(a) versus Figure 15(c), and DN women versus DI women, Figure 15(b) versus Figure 15(d)).

It is interesting to observe the behavior of users in Figures 15(a) and 15(c): these users are the one who use location-aware applications and therefore they should be aware of advantages and disadvantages they incur while using these applications. However, the results show that this is not true: most of them fell "Angry," "Discomfort" and think about "negative consequences," highlighting that the concerns about privacy have increased after seeing what is possible to know about users in a location-aware scenario. This shows that users' knowledge affected users' concerns toward privacy.

To better understand the users' reactions, in the following we analyze users' reactions according to personal profile (public, private) and to privacy settings (changed or not).

Figures 16(a) and 16(b) show the DNs reactions according to the profile type: men with a private or public profile feel "discomfort" or "think about negative consequences"; men with no idea about their profile are "indifferent." The results are different when analyzing the DI group (Figures 16(c) and 16(d)): men with a private profile are "indifferent" but also think about "possible benefits," whereas men with no idea about their profile type fell "discomfort" but also think about "possible benefits." It is interesting to observe the different reactions of men with no idea about personal profile: DNs are "indifferent," whereas DIs think about "personal benefits" or feel "discomfort". DNs have more settled decisions also when analyzing women reactions. Figures 16(b) and 16(d) show that DN women have more negative reactions than DI women. Also in this case, the results show that the concerns about privacy have increased after seeing what is possible to know about users in a location-aware scenario. Indeed, users who

Table 2: User's habits and personal information retrieved by aggregating the 25 most recent generated contents.

User number	Habits	Other personal information
1	Every working day he goes to the train station around 7:30 am, he goes to the cafeteria around 11:30 am and he goes to bed around midnight.	Parents home address.
2	She attends school every morning. She often goes to the "Delfini" public library.	She spent the summer vacation at the seaside. She is good at math and science.
3		He has been to Venice by plane, leaving from the Heathrow airport. While in Venice, he stayed at the Holiday Inn.
4		Personal website address. Personal photo.
5	She goes to school by train.	Favorite TV show: "The Simpsons." She likes ice creams. Departure and arrival train stations.
6	He/she goes to school every morning.	Favorite TV show: "The Blacklist." Favorite band: Coldplay. He/she is good at Latin, but not at Math. Cellphone operator.
7	She goes to school every morning.	She is not good at Math. Cellphone operator. Uncle name. She is attending the fourth year at the high school. She recently went to London.
8	She goes to work every morning.	Cellphone brand. Place where she eats every working day. Personal photo. She loves skiing. Favorite TV show: "X-Factor." Personal photo.
9	She goes to school every morning.	Favorite TV show: "Scrubs."
10	He goes to school every morning.	He is a soccer fan. He is seeing a girl. Photo of the girl he is seeing. He is not good at Chemistry. Last Saturday he and his girlfriend went to a grill restaurant.

set their profile as public or do not remember the profile type should be not concerned about privacy, but results show the opposite. A better knowledge of the location-aware scenario affected their privacy concerns.

Figure 17 shows the DNs reactions according to privacy settings changes. In general, DN men are more worried than DI men. Similarly, DN women are more worried than DI women, with the exception of women who have no idea about changing their privacy settings: DI women gave more "angry" and more "think about negative consequences" answers. Within the DN group, women are more worried than men; the same happens within the DI group, but the difference between men and women is less great. Similarly to the previous analysis, users who did not change, or do not remember changing, their privacy settings should be not concerned about privacy, but the results show that a better knowledge of the location-aware scenario affected their privacy concerns.

The second question investigates the user's willing to be contacted by third parties according to the location extracted from contents publicly available. Figure 18 reports results obtained when considering users who claim to use location-aware services and when considering users who claim not to use these services. Results show that DN and DI members do not want to be contacted, regardless they use location-aware applications or not. However, users (either DNs or DIs) who use location-aware applications are more willing to be contacted provided some constraints are met. For instance, around 40% of DNs who use location-aware services require third parties to be authorized; 45% of DI men require to receive personal benefits, whereas 30% of DN men are willing to be contacted if they can be of any help. DN men who claim not to use location-aware services are more willing to be contacted than women. Note the high percentage of users who do not want to be contacted among DI members who claim not to use location-aware services.

In the following we analyze the users who will to be contacted according to personal profile (public, private) and to privacy settings (changed or not).

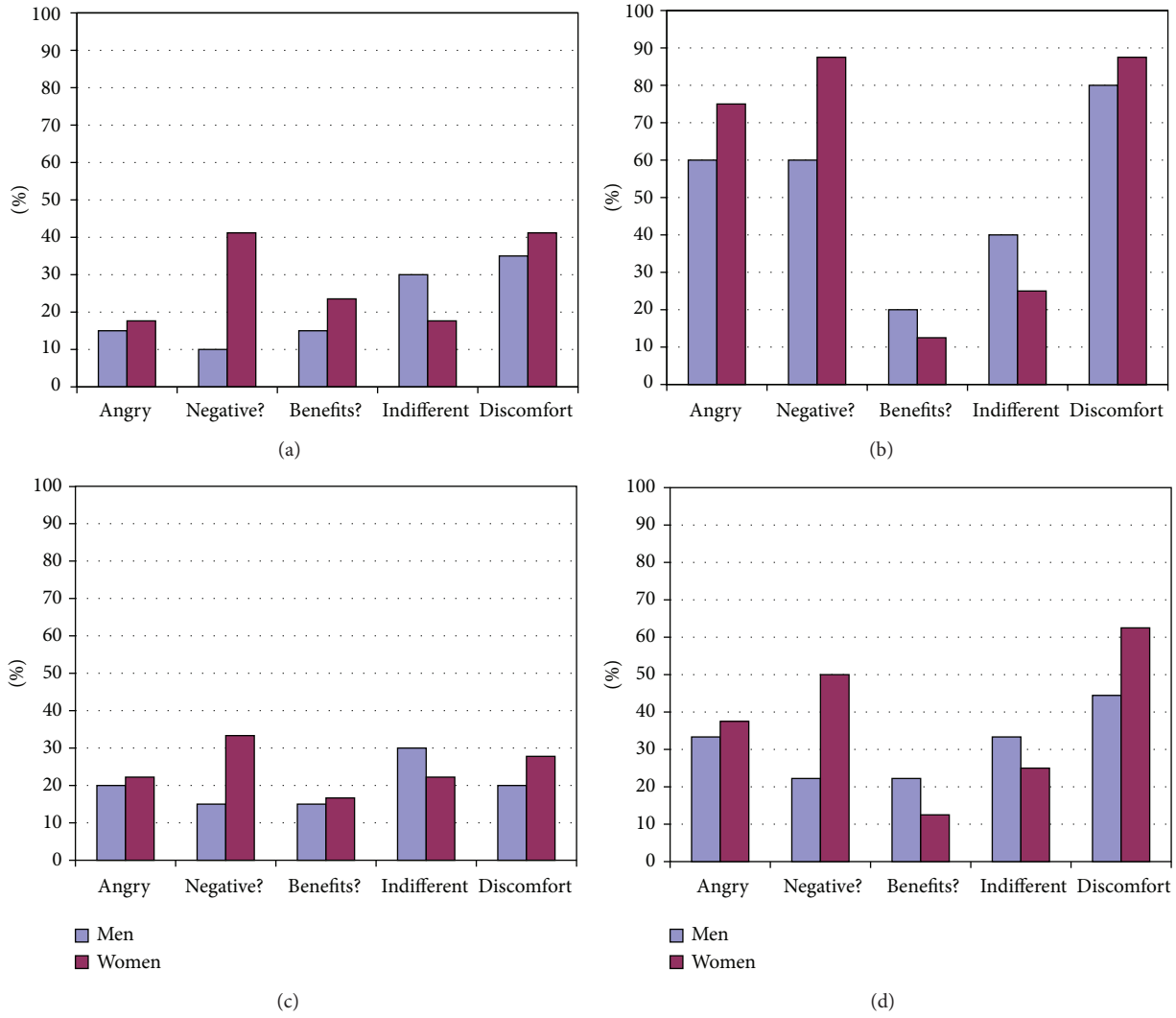


Figure 15: Users reaction if third parties would access their personal location: (a) DNs who claim to use location-aware applications; (b) DNs who claim not to use location-aware applications; (c) DIs who claim to use location-aware applications; (d) DIs who claim not to use location-aware applications.

Figure 19 shows the users' will to be contacted according to the profile type. Results show that DN men are willing to be contacted if they authorize third parties or if they can be of any help for someone; DN men with no idea about their profile also think about personal benefits. DI men with private or public profile are willing to be contacted if they receive benefits (either personal or for someone else) and if they authorize third parties; DI men with no idea about the profile prefer not to be contacted, but they are willing to be contacted if they receive benefits or if they authorize third parties. Among women, DIs are more willing to be contacted than DNs. To be contacted, both groups require third parties to be authorized or to provide benefits.

Figure 20 shows the users will to be contacted according to privacy settings changes. Similarly to the previous analysis, users are willing to be contacted if they can receive benefits or if they authorize third parties.

The third question asks users to define a location-aware service able to contact them according to the location extracted from contents publicly available. Figure 21 reports results obtained when considering users who claim to use location-aware services and when considering users who claim not to use these services. Results show that DNs who claim to use location-aware applications define the service as "Intrusive" (59% for men and 40% for women), but also find the service "Interesting" (29% for men and 30% for women). DNs who claim not to use location-aware applications define the service as "Intrusive" (60% of men and 87% of women), "alarming" (20% of men and 37% of women). It is interesting to note that 80% of men who claim not to use location-aware applications define the service as "Interesting." DIs who claim to use location-aware applications define the service as "Intrusive" (20% for men and 56% for women), but 45% of the DI men find the service "Interesting." DI

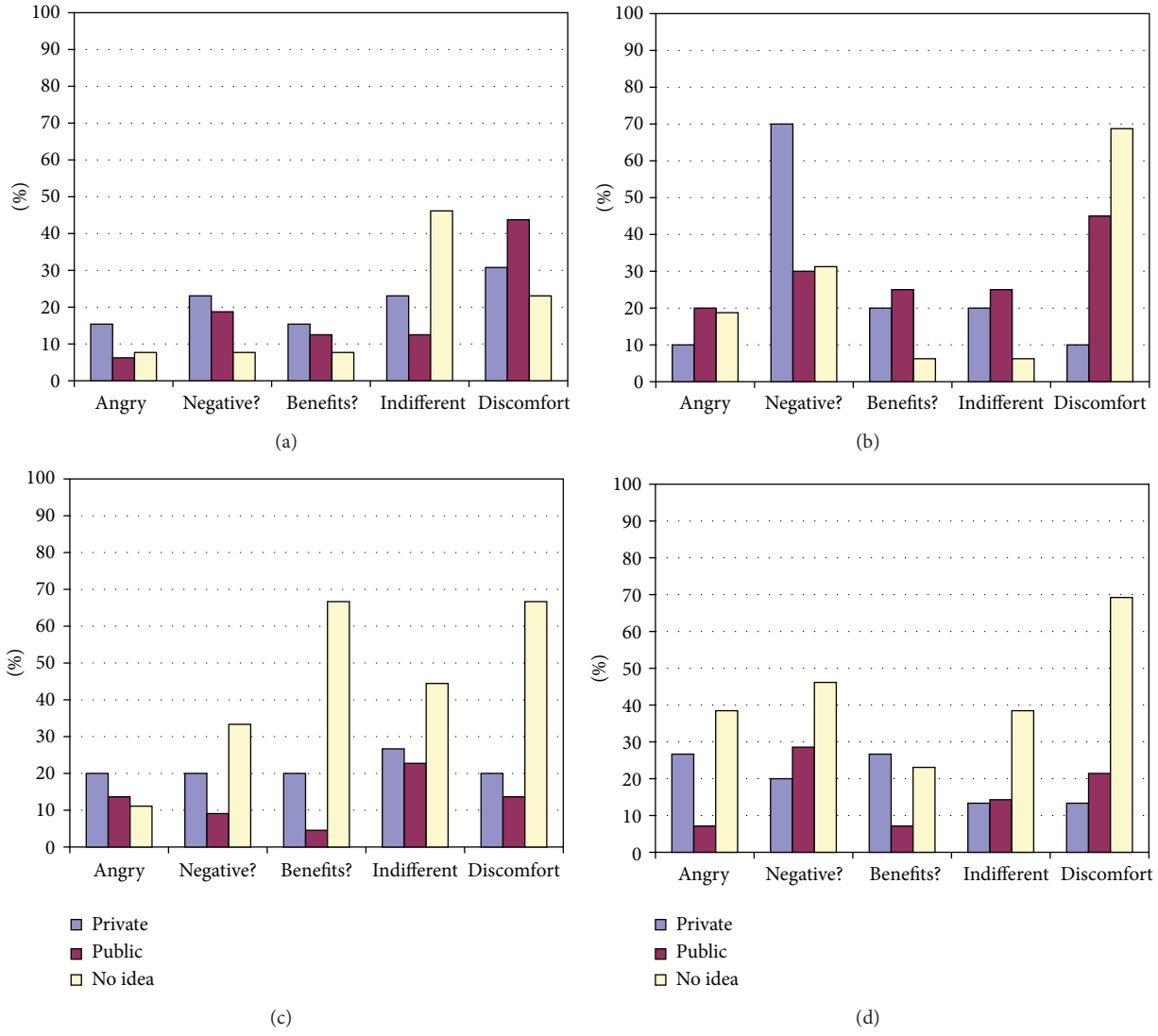


Figure 16: Reaction to be contacted according to the profile type: (a) DNs men; (b) DNs women; (c) DIs men; (d) DIs woman.

users who claim not to use location-aware applications define the service as "Intrusive" (67% of men and 88% of women), "alarming" (44% of men and 50% of women). "Interesting" is the definition provided by 37% of DI women and 22% of DI men.

Although most of the respondents negatively define the service, several positive feeling options were checked. This attitude can be explained mainly by the fact that the deployment of location-aware applications is still in its infancy. Most users do not know or have not yet experienced this type of services and, therefore, the advantages arising from these services are not well known. Some researchers (e.g., [8]) argue that concerns about privacy tend to decrease when subjects begin to appreciate the benefits of these applications.

Figure 22 shows the users' definition according to the profile type. Results show that men with a private or public profile define the service as "Interesting," whereas men with no idea about their profile define the service as "Intrusive." Women give different definitions as the majority of them define the service as "Intrusive" or "Alarming." DI men are more alarmed than DN men. DN women are more interested than DI women.

Figure 23 shows the users' definition according to privacy settings changes. Results show that DN men find the service "Intrusive," but also "Interesting," whereas DI men also find the service "Alarming." DN women define the service as "Intrusive" and "Alarming." DI women who changed their privacy settings define the service as "Interesting" and "Alarming." DI men are less interested than DN men. DI women are more alarmed but also more interested than DN women.

4.3. Summary of Results and Main Findings. The goal of the second part of the investigation was to understand users' opinion toward location-aware services that may extract personal and sensitive information from contents publicly available in social media platforms. Since the location-aware

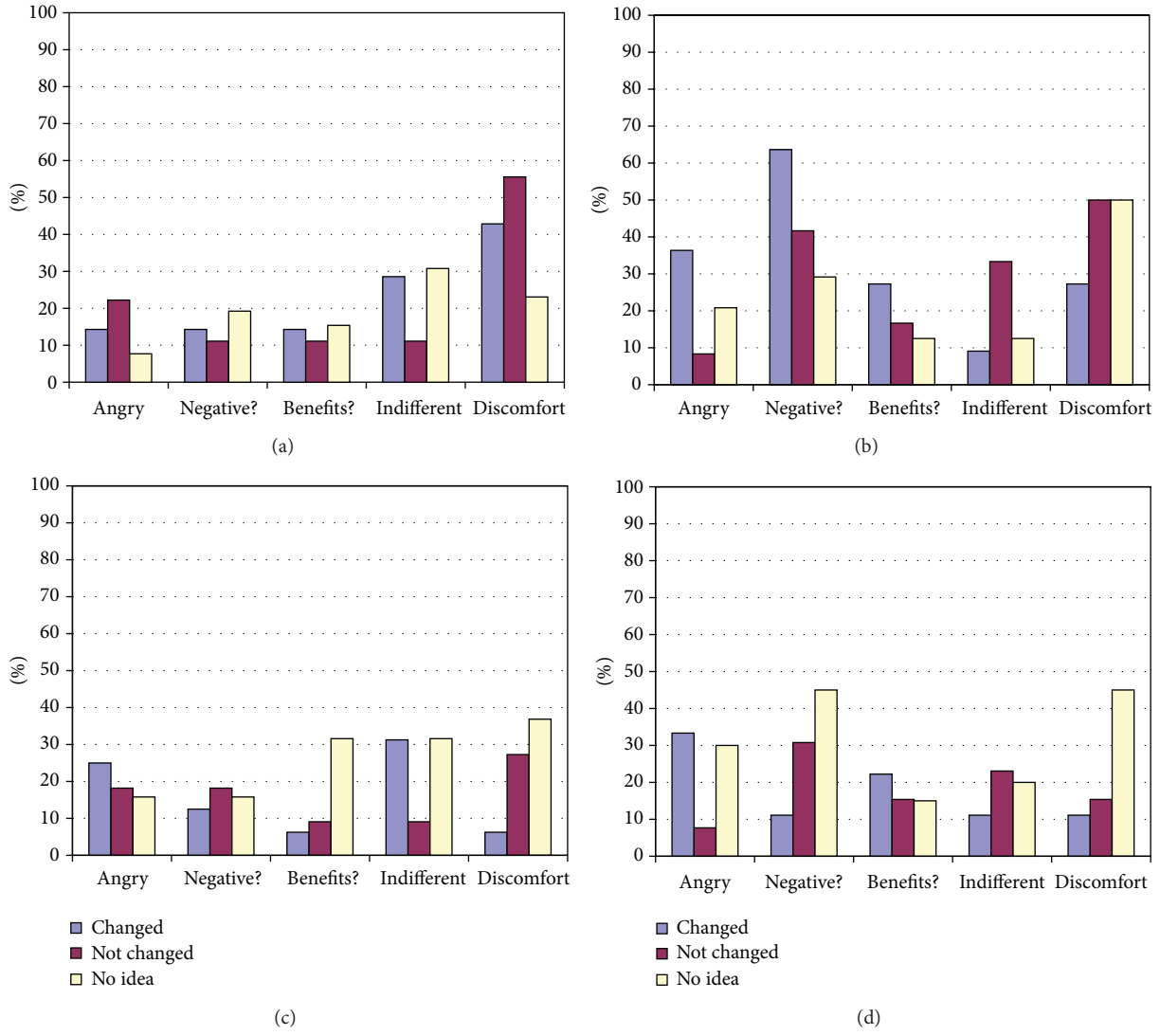


Figure 17: Reaction to be contacted according to privacy settings changes: (a) DN men; (b) DN women; (c) DI men; (d) DI woman.

scenario is in its infancy stage, before asking for their opinions, we showed users a simple application in order to aware them of the power of location-aware services and therefore with the goal of reducing the lack of knowledge that would likely affect the obtained results.

According to the obtained results users who use location-aware services are less worried and concerned about the scenario, whereas users who claim not to use location-aware services are alarmed. In general, although the reactions of DNs are more negative than the ones of DIs, DNs are interested in the location-aware and are more willing to be contacted than DIs.

In summary, the second part of the investigation highlights:

(i) Users' reactions: DNs are more worried and concerned that DIs about these services. Within the groups, DN women are more worried than DN men and the same happens within the DI group, although the difference is less great. We expected users of location-aware applications to react in a positive way, but the results showed that most of these users fell "Angry", "Discomfort" and think about "negative consequences". This confirms the hypothesis that users' knowledge affected users' concerns toward privacy: concerns about privacy have increased after seeing the personal and sensitive information that is possible to extract from contents publicly available in a location-aware scenario.

(ii) Users' willing to be contacted: both groups agree that they do not want to be contacted by third-party services according to the position. However, a considerable number of participants are willing to be contacted if some constraints are met: provide authorization, receive personal benefits or be of any help to someone. In general, DN members are more willing to be contacted by third parties according

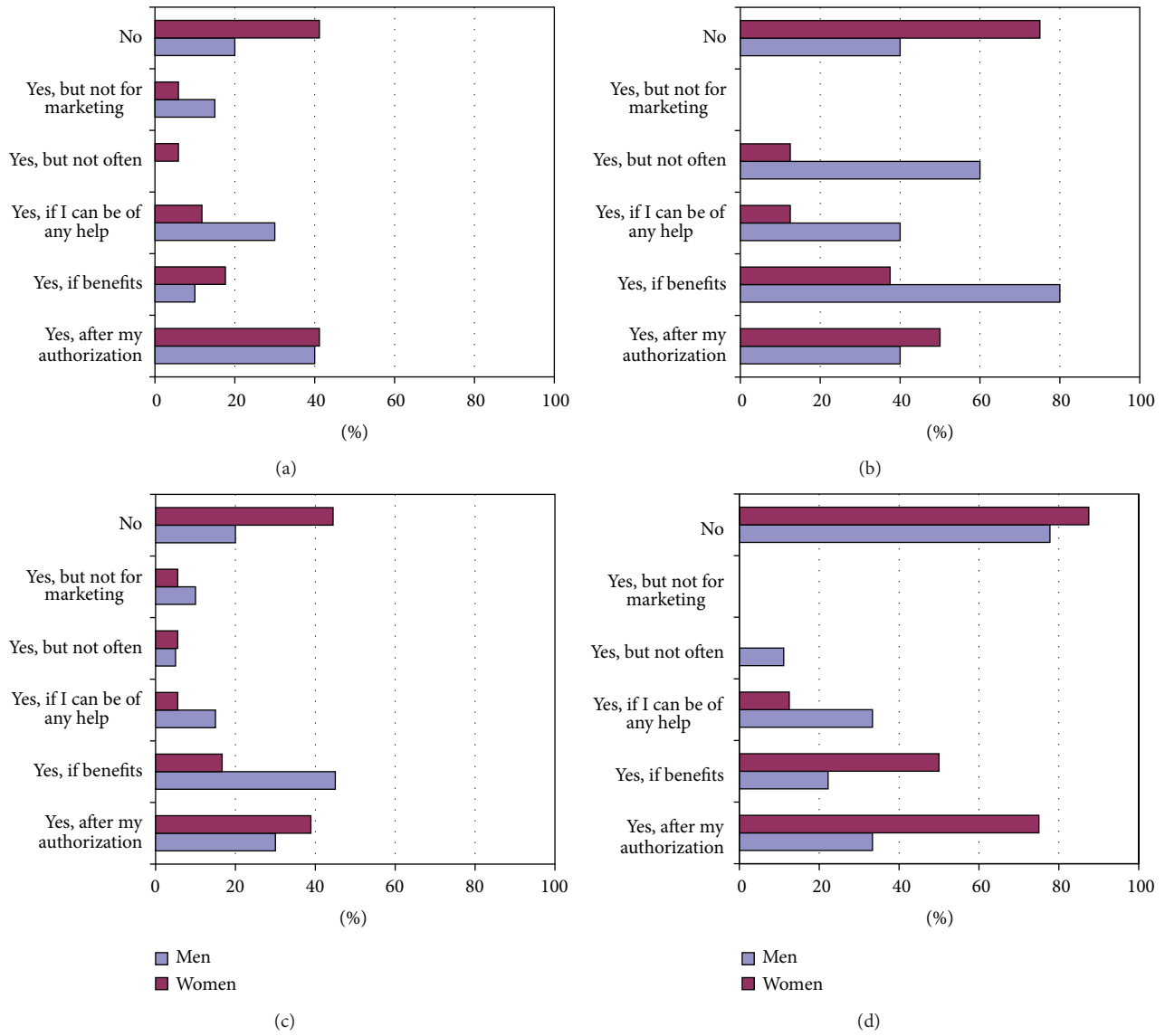


Figure 18: Will to be contacted according to the tweet or photo location: (a) DN who claim to use location-aware applications; (b) DN who claim not to use location-aware applications; (c) DI who claim to use location-aware applications; (d) DI who claim not to use location-aware applications.

to their geographical location, DI members think of their own possible benefits whereas DN also think of benefits for someone else.

(iii) Users' definition: both groups define a third-party service able to contact users according to the tweet or photo location as "Intrusive", but DNs are also interested to the service; conversely, DIs are more alarmed.

5. Guidelines to Develop Effective Location-Aware Services

Location-aware services are changing the way users conduct business and free time: over the next ten years, the market is estimated at more than US$100 billion in revenue to service providers and as much as US$700 billion in value to consumer and business end-users [20]. The results of our investigation showed that DNs and DIs are ready to enter into the location-aware scenario from the technological point of view, but also showed that their knowledge about the scenario is poor: users are not completely aware of, or tend to forget, what may happen to the contents they produce and share over social media platforms. Indeed, the results showed that users' knowledge affect users' concerns toward privacy: after showing users that location-aware services can produce an accurate personal profile with activities and habits, the concerns toward privacy increased also among users who say they regularly use location-aware services. Needless to say, users' concerns toward privacy may limit the success of future location-aware services. For this reason, it is necessary to ameliorate these concerns.

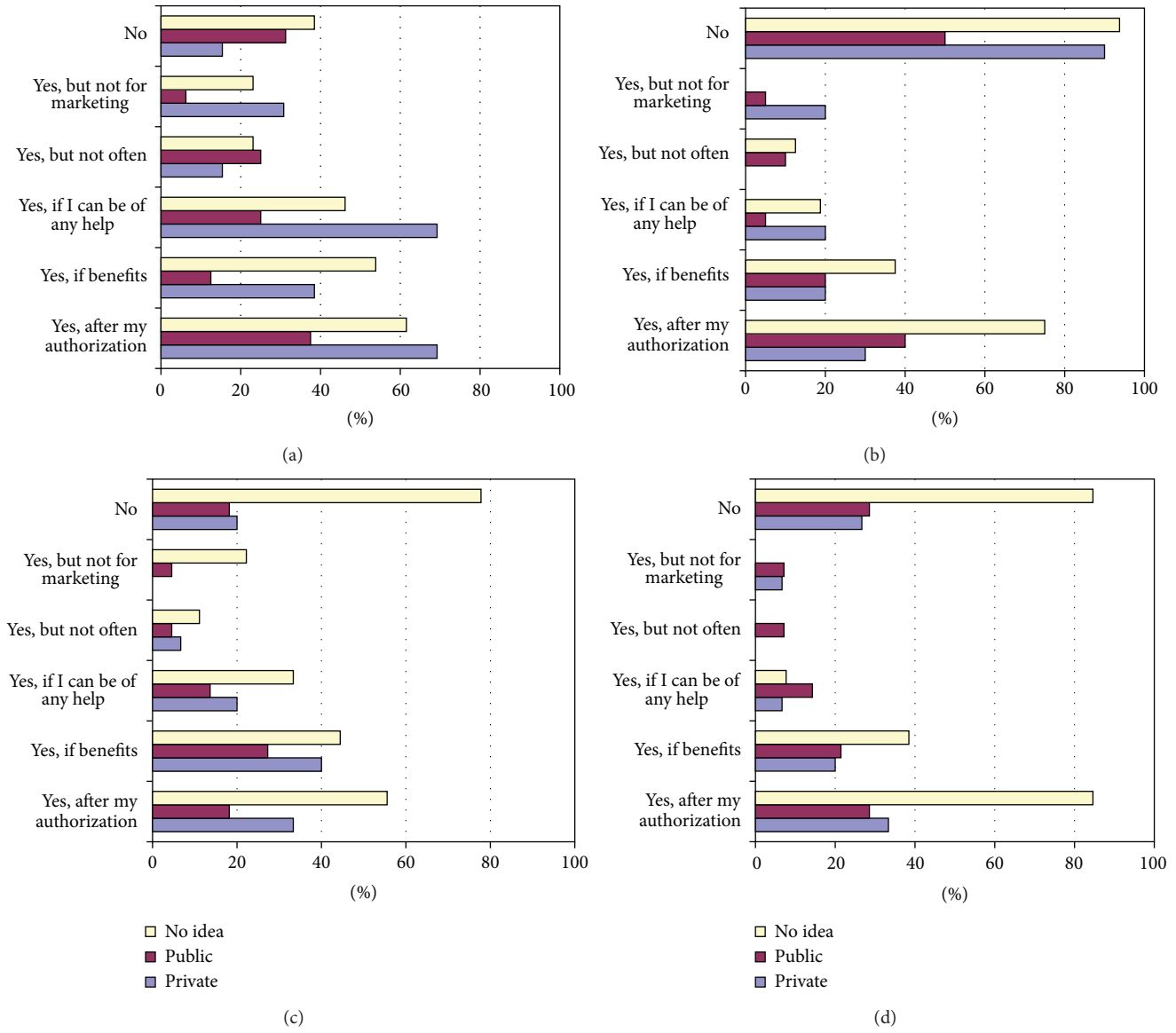


Figure 19: Will to be contacted according to the profile type: (a) DN men; (b) DN women; (c) DI men; (d) DI woman.

There are many players involved in the location-aware scenario (e.g., developers, service providers, advertisers, users, and application markets) and, therefore, the protection of the location privacy cannot be made by the sole domain of technologist or policy makers. Rather, it is necessary that all the players involved in the scenario participate in the protection of the users' privacy. In the following, we use the results obtained from our investigation, to provide guidelines for two players involved in the location-aware scenario: developers and users.

5.1. Developers. Developers of location-aware applications play a critical and challenging role in the development of a successful location-aware scenario: collecting as many data as possible is tempting for many developers, but this may increase users' concerns and may affect the commercial success of the developed application. Indeed, developers decide not only what personal data to collect, but also how, where, and why to collect these data. Moreover, they also decide to whom these data can be disclosed.

In the following, we propose guidelines that might help developers to find the right balance between the user's privacy and the success of the application.

(1) Location privacy: developers should describe the privacy policy under which the location data is being collected, stored, and disclosed. The description should be clear, concise, and effective (e.g., important information should be easily accessible, whereas details should be provided through links so that users who want more details can easily access these documents).

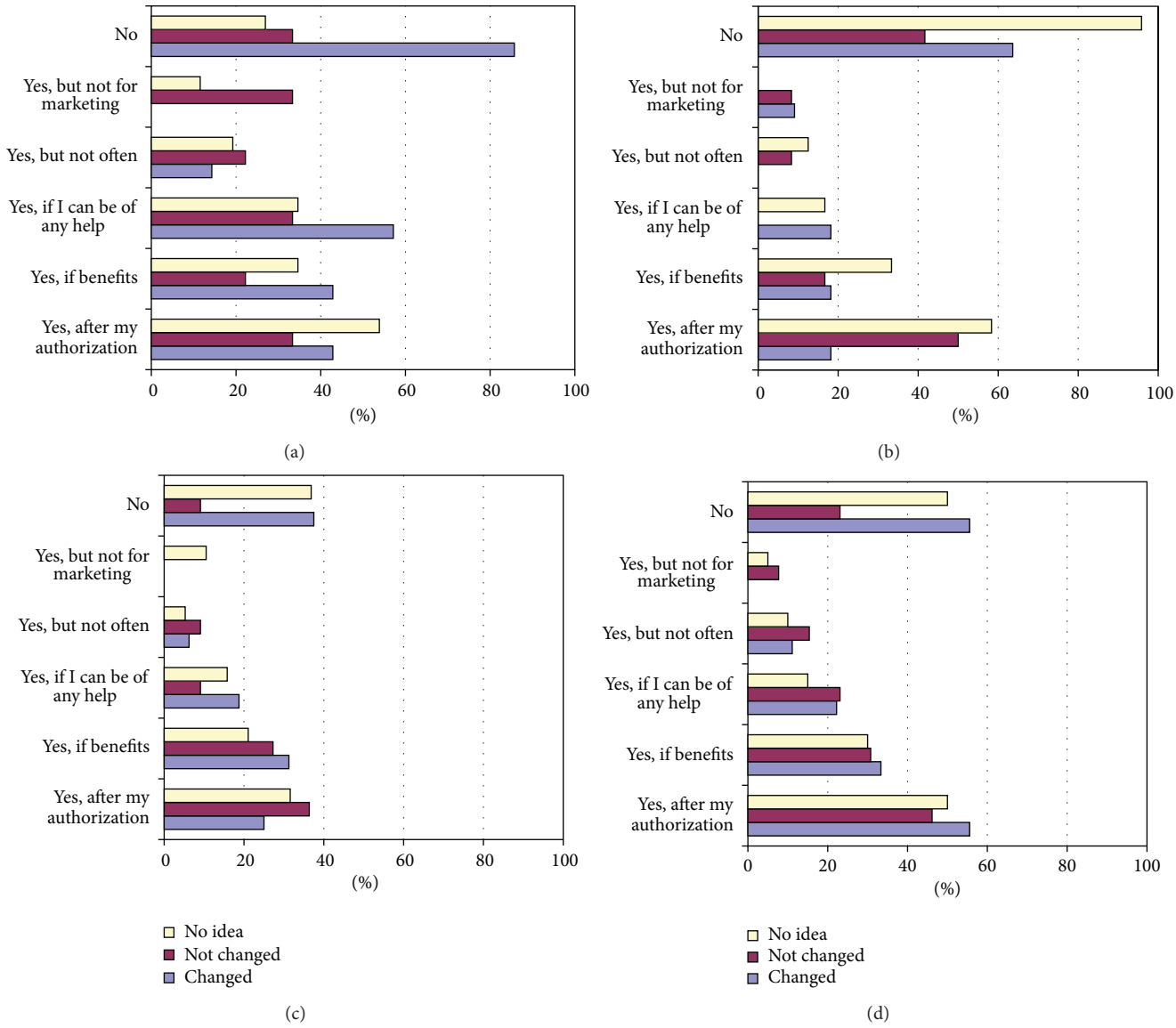


Figure 20: Will to be contacted according to privacy settings changes: (a) DN men; (b) DN women; (c) DI men; (d) DI woman.

(2) On-the-fly protection: developers should provide users with the ability of protecting their location privacy on-the-fly: in addition to the location enable/disable feature available at application level, the application should give users the ability to control/protect these pieces of information at disclosing time (e.g., when user generated contents are shared in social media platforms). For instance, users should be able to mask their geographical position when producing a content (e.g., developers might use technologies like geographical masking or cloaking to modify the geographical coordinates associated with the original data with the introduction of a random noise or to use a spatiotemporal low resolution). The use of pop-up messages may be useful: for instance, a message like "Your location is hidden in the data you are posting, Continue, mask or remove info?" would be very informative for the users. Alternatively, the application might use a symbol to raise user awareness. Similarly, if multimedia contents are involved, the application should clearly state what are the hidden tags that will be available to everyone and it should give the users the ability to remove these pieces of information.

(3) Data collection and management: developers should inform users of every collected type of data, their usage, and their possible disclosure to third parties (e.g., the applications should never activate the camera or collect user's locations or movement sensors without the permission of the user); developers should provide users with the ability of accessing/deleting all of the data collected about them: a user might modify personal information and privacy

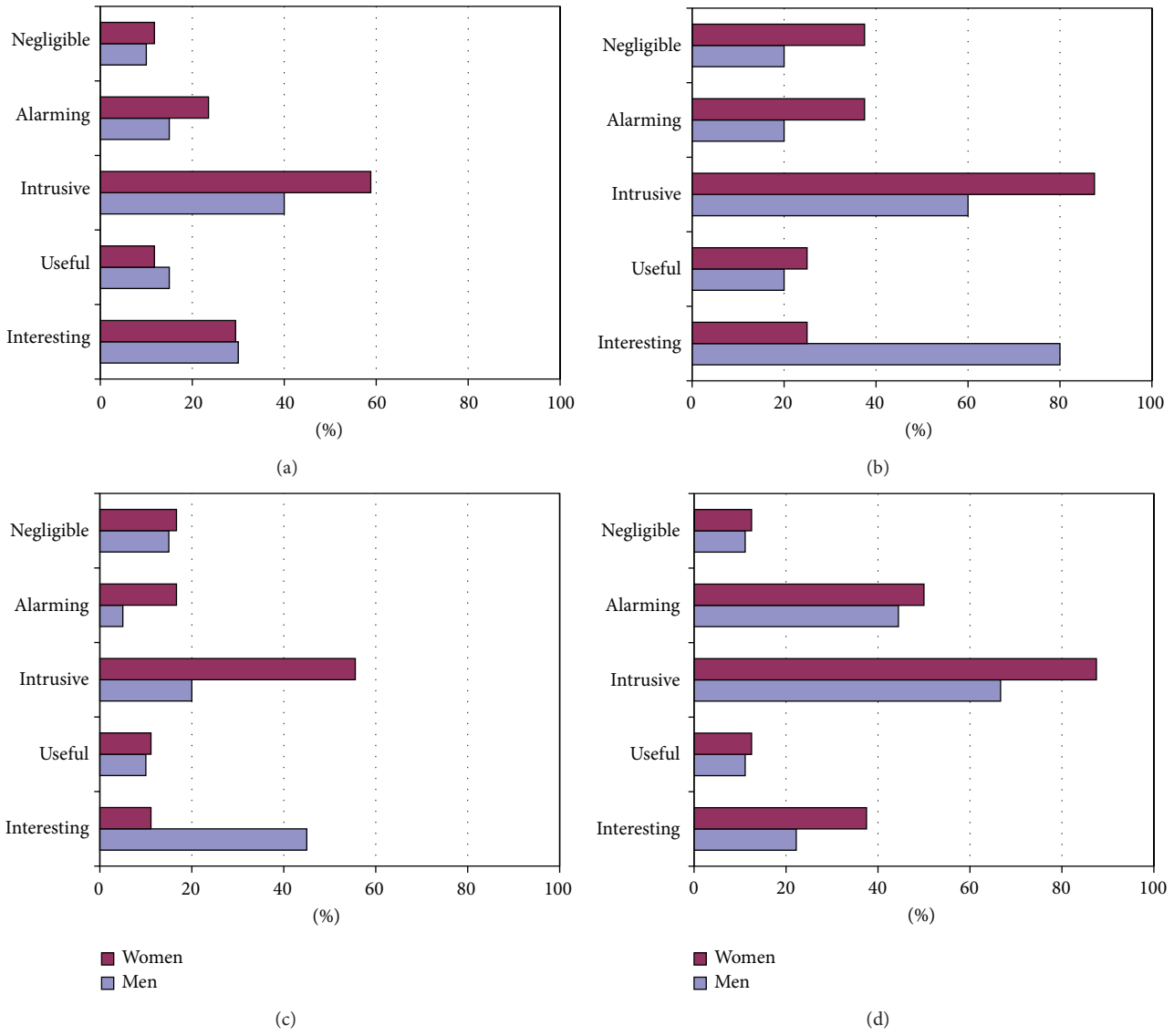


Figure 21: Definition of a service able to contact users according to the Tweet or photo location. (a) DN who claim to use location-aware applications; (b) DN who claim not to use location-aware applications; (c) DI who claim to use location-aware applications; (d) DI who claim not to use location-aware applications.

options whenever he/she wants, and when a user deletes the application, his/her personal data should also be deleted automatically.

(4) Data validity: the user's consent should be renewed after a period of time. Currently, the consent is asked at download/installation time and it lasts forever. It is difficult for users to remember the privacy policy and the data collection for every application.

(5) Transparency: changes to privacy policy, data collection, usage, management, and validity should be communicated to users in a clear, concise, and accurate form. The application should inform exactly about rules that have been modified, so it is easy for users to understand the novelty. Furthermore, the communication should be given in advance, in order to give users a reasonable time to evaluate the changes. Silent updates should definitely be avoided.

5.2. Users. Users should be aware that they have a key role in protecting their privacy: they are responsible for the personal information collected and used and disclosed through the used applications. For this reason, they should learn advantages and disadvantages of technologies and they should think carefully before posting or tagging personal information. In the following, we propose guidelines that might be helpful to users when operating in a location-aware scenario.

(1) Privacy policy: users should read the privacy policy before giving consent at download time. Furthermore, users should periodically check the privacy policy in order to understand if something changed.

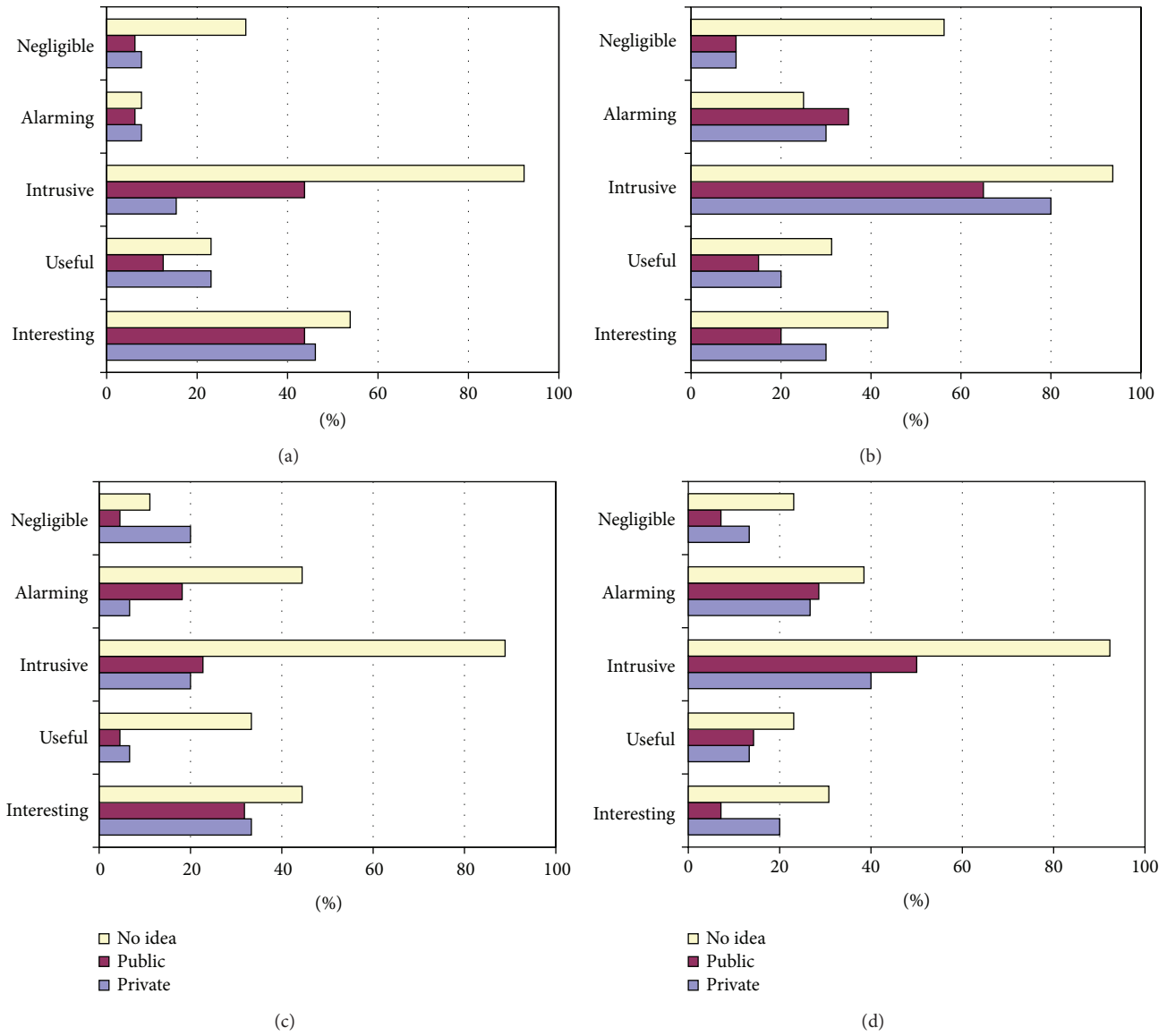


Figure 22: Definition given according to the profile type: (a) DN men; (b) DN women; (c) DI men; (d) DI woman.

(2) Device knowledge: users should be aware of the technologies available in their device and should know advantages and disadvantages of using these technologies. Furthermore, they should know how to enable/disable specific services and/or technologies.

(3) Applications knowledge: users should be aware of what data the installed applications have access to and of what data the applications collect.

(4) Notifications: user should read every pop-up notification and should think about possible consequences before accepting or denying a request.

(5) Sharing data: users should be aware that user generated contents are usually coupled with hidden data that contain user's personal information (e.g., location data). Therefore, they should check what data the application hides: if they are comfortable with that, they may proceed to the sharing; otherwise it is better not to share contents (e.g., is the user comfortable if everybody knows where and when he/she took a picture?).

6. Conclusions

Several studies focused on users' privacy in location-aware services, but results did not clarify if users are concerned or not. In our opinion, this is mainly due to the infancy stage of the location-aware scenario and to the methodology used to investigate users' attitudes and opinions toward privacy in a location-aware scenario. For this reason, in this paper we proposed a different approach to investigate privacy concerns toward location-aware services. Our hypothesis is that users' knowledge affects users' privacy concerns. Therefore, we conducted our analysis in two separate steps: (i) the initial

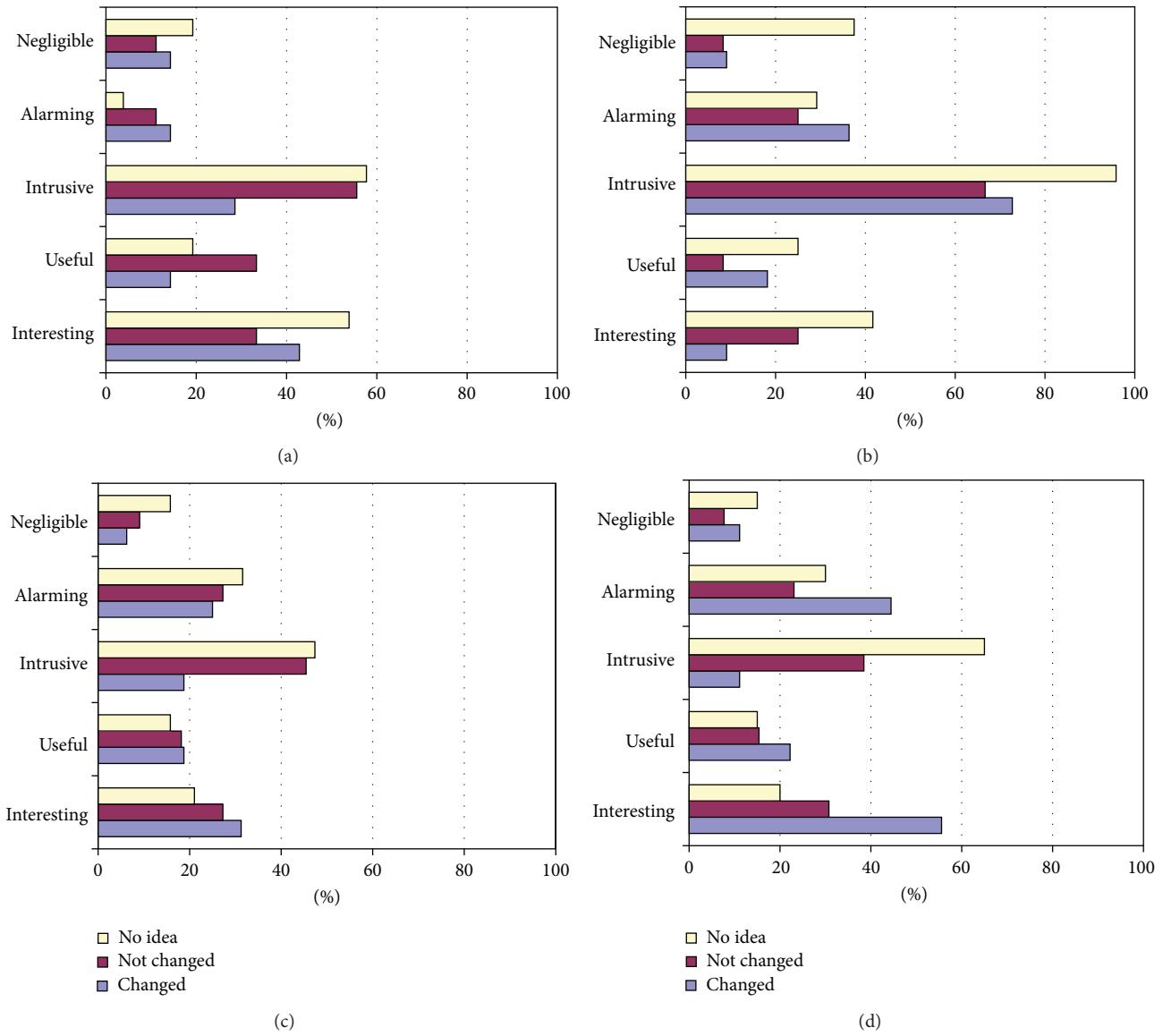


Figure 23: Definition given according to privacy settings changes: (a) DN men; (b) DN women; (c) DI men; (d) DI woman.

step investigated the knowledge users have on the location-aware scenario; (ii) the second step investigated users' opinions toward location-aware services, but the investigation has been done after showing users examples of personal and sensitive information that can be extracted from social media platforms by a developed location-aware application. Moreover, to get insights of what may happen in future location-aware scenarios, our study separately analyzed the behavior of digital natives and of digital immigrants; indeed, digital natives are usually considered early adopters of new technologies and services and therefore their current behavior may reflect what will happen in the near future.

The obtained results showed that users install location-aware applications over their devices without any concern but also highlighted that users ignore many of the features of location-aware services as well as they do not remember accessing privacy settings. In few words, it looks like that users are not really concerned about privacy. However, the second part of the investigation confirmed our hypothesis that users' knowledge affects users' concerns toward privacy: concerns about privacy have increased after seeing the personal and sensitive information that is possible to extract from contents publicly available in a location-aware scenario. The analysis also revealed that DNs are more interested in the location-aware scenario and that users' concerns toward these services may be ameliorated if users are asked for authorization and are provided with benefits. This and other findings were used to outline possible guidelines that might be helpful to develop effective location-aware services.

Conflict of Interests

The author declares that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

The author would like to thank Valentina Tamanini for the initial analysis of the location-aware scenario.

References

[1] K. P. N. Puttaswamy, S. Wang, T. Steinbauer et al., "Preserving location privacy in geosocial applications," *IEEE Transactions on Mobile Computing*, vol. 13, no. 1, pp. 159–173, 2014.

[2] S. Ferretti, M. Furini, C. E. Palazzi, M. Roccetti, and P. Salomoni, "WWW recycling for a better world," *Communications of the ACM*, vol. 53, no. 4, pp. 139–143, 2010.

[3] M. Roccetti, S. Ferretti, C. E. Palazzi, M. Furini, and P. Salomoni, "Riding the web evolution: from egoism to altruism," in *Proceedings of the 5th IEEE Consumer Communications and Networking Conference (CCNC '08)*, pp. 1123–1127, January 2008.

[4] M. Furini, "Mobile games: what to expext in the near future," in *Proceedings of the GAMEON Conference on Simulation and AI in Computer Games*, EuroSis Society, November 2007.

[5] H. Li, H. Hu, and J. Xu, "Nearby friend alert: location anonymity in mobile geo-social networks," *IEEE Pervasive Computing*, vol. 12, no. 4, pp. 62–70, 2013.

[6] S. Consolvo, I. E. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. 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)*, pp. 81–90, ACM, April 2005.

[7] L. Barkus, "Privacy in location-based services, concern vs. coolness," in *Proceedings of the 2004 Workshop on Location System Privacy and Control*, 2004.

[8] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Measuring user confidence in smartphone security and privacy," in *Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS '12)*, pp. 1: 1–1: 16, ACM, 2012.

[9] P. G. Kelley, M. Benisch, L. F. Cranor, and N. Sadeh, "When are users comfortable sharing locations with advertisers?" in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*, pp. 2449–2452, ACM, May 2011.

[10] D. Fisher, L. Dorner, and D. Wagner, "Short paper: location privacy: user behavior in the field," in *Proceedings of the 2nd ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM '12)*, pp. 51–56, ACM, 2012.

[11] E. J. Helsper and R. Eynon, "Digital natives: where is the evidence?" *British Educational Research Journal*, vol. 36, no. 3, pp. 503–520, 2010.

[12] L. Jedrzejczyk, B. A. Price, A. K. Bandara, and B. Nuseibeh, "On the impact of real-time feedback on users' behaviour in mobile location-sharing applications," in *Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS '10)*, pp. 14: 1–14: 12, July 2010.

[13] N. Sadeh, J. Hong, L. Cranor et al., "Understanding and capturing people's privacy policies in a mobile social networking application," *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 401–412, 2009.

[14] J. S. Olson, J. Grudin, and E. Horvitz, "A study of preferences for sharing and privacy," in *Proceedings of the Extended Abstracts on Human Factors in Computing Systems (CHI EA '05)*, pp. 1985–1988, ACM.

[15] L. Palen and P. Dourish, "Unpacking "privacy" for a networked world," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '03)*, pp. 129–136, ACM, April 2003.

[16] S. Lederer, I. Hong, K. Dey, and A. Landay, "Personal privacy through understanding and action: five pitfalls for designers," *Personal and Ubiquitous Computing*, vol. 8, no. 6, pp. 440–454, 2004.

[17] T. Burghardt, E. Buchmann, J. Muller, and K. Bohm, "Understanding user preferences and awareness: privacy mechanisms in location-based services," in *Proceedings of the Confederated International Conferences, CoopIS, DOA, IS, and ODBASE 2009: On the Move to Meaningful Internet Systems: Part I (OTM '09)*, pp. 304–321, Springer, Berlin, Germany, 2009.

[18] S. Ahern, D. Eckles, N. Good, S. King, M. Naaman, and R. Nair, "Over-exposed? Privacy patterns and considerations in online and mobile photo sharing," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '07)*, pp. 357–366, ACM, May 2007.

[19] A. Walker and O. Zur, *On Digital Immigrants and Digital Natives: How the Digital Divide Affects Families, Educational Institutions, and the Workplace. Research Report*, Zur Institute, 2011.

[20] J. Manyika, M. Chui, B. Brown et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity. Research Report*, McKinsey Global Institute, 2011.