Metrics for Privacy Assessment When Sharing Information in Online Social Networks

JOSE ALEMANY[1], ELENA DEL VAL [ID][2], JUAN M. ALBEROLA[1,3], AND ANA GARCÍA-FORNES[1]
[1]Universitat Politècnica de València, 46022 Valencia, Spain
[2]Departamento de Informática e Ingeniería de Sistemas, Universidad de Zaragoza, Escuela Universitaria Politècnica de Teruel, 44003 Teruel, Spain
[3]Florida Universitària, 46470 Valencia, Spain

Corresponding author: Elena del Val (edelval@unizar.es)

ABSTRACT Privacy risk in Online Social Networks has become an important social concern. Users, with different perceptions of risk, share information without considering the audience that has access to the information disclosed or how far a publication will go. According to this, we propose two metrics (Audience and Reachability) based on information flows and friendship layers that indicate the privacy risk of sharing information, addressing the posts' scope and invisible audience. We assess these metrics through agent simulations in well-known models of networks. The findings show a strong relationship between metrics and structural centrality network properties. We also studied scenarios where there is no previous information about users activity or the information about the traces of the messages cannot be obtained. To deal with privacy assessment in these scenarios, we analyze the relationship between the proposed privacy metrics and local centrality properties as an estimation of privacy risk. The results showed that effectiveness centrality can be used as a suitable approximation of the proposed privacy measures.

INDEX TERMS Privacy, information sharing, social networks, network topology.

I. INTRODUCTION

One of the most common online activities in the European Union in 2014 was participation in social networking [13]. According to Eurostat [21] nearly half (46 %) of individuals aged 16 to 74 used the Internet for social networking (i.e., using sites such as Facebook or Twitter). In general, the number of social network users is increasing and it will reach the 2.72 billion in 2019 [11].

There are many users of social networking sites who are not aware of privacy and often share information without considering who will or will not have access to it [22]. The effect of the lack of privacy awareness led users to negative experiences related to privacy [40], and in some cases, there are users who consider leaving as a consequence of inadequate control over their data [10].

Regarding problems with privacy awareness and privacy settings configuration in Online Social Networks (OSNs), the provision of metrics and mechanisms that facilitate the management of individuals' privacy and enhance the awareness of privacy risks become an important issue [39],

The associate editor coordinating the review of this manuscript and approving it for publication was Haipeng Yao [ID].

[46]. Applications related to OSN usually provide mechanisms to configure the users' privacy profile. Nevertheless, the majority of approaches focus on protecting the information referred to user profile and not to the visibility of his/her publications. In the literature we can find proposals that try to address these issues with the automation of privacy settings [6], [14], [38]. However, these usually require some intervention from the user and do not solve the problem of increasing privacy awareness. Other works deal with the improvement of user's awareness about the misalignment of users' expected audience with the actual audience [8], [23], [29]. These latter works facilitate the alignment between the expected and the actual audience. However, there is still an open problem. These proposals do not take into account that users that are part of the target audience might re-share the published information, losing control over the original publication scope.

The structure of the network is one of the main factors that have influence on the scope of a sharing action [19]. This scope can be seen as the effect of a message diffusion process. Spreading processes such as epidemics or information diffusion have been analyzed in the area of Complex Networks [25], [27]. Several works have studied spreading

dynamics and influential or relevant individuals in these processes [34], [43].

In social networks, the concept of influential users are referred to those users strategically located in the network, which are responsible of information diffusion since they can efficiently and conduct the dissemination of a message. Since influential users may contribute to increase the privacy risk [24], determining if there are influential users in the path that a user's publication follows would be essential to assess the privacy risk of this publication. Related to this issue, it is widely accepted that structural metrics such as degree [33], PageRank [28], closeness, or betweenness [16]–[18], [26] are suitable to detect influential users [7].

The perception of risk may be different from one user to another [9], [30], [36]. Some users are more comfortable with the possibility that their publications can be seen by others and they may be even interested in achieving that effect. In contrast, other users prefer not to disclose their information beyond their direct friends [15]. Therefore, different levels of risk perception should be considered for determining the privacy risk.

Unlike other proposals that present mechanisms to facilitate the alignment between the expected and the actual audience, in this article we focus on the analysis of the potential reach of a publication in social networks as a consequence of re-sharing actions, assuming that the publication was received by the expected audience. We present two privacy metrics: Reachability for measuring the user posts probability to reach certain depth level; and Audience for clarifying the invisible audience, measuring the percentage of users that really will access to posts. The metrics act as an indicator of the potential risk of user's actions, and are based on information flows and a friendship-layered model that provides information about the reachability of a user publication based on the distance between the user and the potential audience. Finally, to consider scenarios where third applications cannot have access to the traffic of users' messages in online social networks, we analyze if there is a correlation between structural network factors and the proposed metrics. The results obtained in the experiments conclude that local structural properties are correlated with the proposed privacy metrics.

The paper is organized as follows. Section 2 presents previous approaches related to privacy score metrics. Section 3 exposes the privacy risks in social networks with a usual scenario and proposes a solution. Section 4 describes the proposed layered privacy risk metrics. Section 5 presents the experiments that analyze if there is a correlation between structural properties and the proposed privacy metrics. Finally, section 6 presents conclusions.

II. RELATED WORK

As communication through social networks acquires greater relevance in our daily social interactions, it is important that users understand the effect of communicative actions using these social tools. Users often see OSN as tools that facilitate communication that has traditionally been face-to-face [2].

However, communication using OSN does not have the same impact as traditional communication. It is important for users to be aware of the scope of their communicative actions through OSN [20], [35].

Previous works tried to deal with this problem from different perspectives. There are approaches that provide wizards to facilitate the management of privacy profile settings. Fang and LeFevre [14] present a privacy wizard based on an active learning paradigm. Users can assign ''labels'' (i.e., share or not share) to a set of selected friends. Then, previous labelling processes are used as the input for their classifier. Finally, this wizard determines labels for the remaining friends of these user that are in the same circle. However, this approach assumes that friends in the same social circle have show similar responses of sharing publications. Thus, this approach does not consider that friends can play different roles. Liu and Terzi [50] propose a privacy score based on user's profile items but without considering the dynamics of how an information item is re-shared through the social network. The authors also propose a recommendation based on a comparison between the user's privacy score and his/her neighbors score. If the score is below that of his/her neighbors, the system can recommend stronger privacy settings. However, not all users in a social network have the same perception of privacy risk. Therefore, a recommendation based only on your neighbors could not fit to your privacy preferences. A privacy score is also proposed by Vidyalakshmi *et al.* [38]. The authors present a framework for obtaining a privacy score metric from an individual perspective. This metric considers users' personal attitude towards privacy and communication information. Privacy score is estimated using cubic bezier curve that integrates: (i) user's disposition to privacy; (ii) user's attitude towards communication; (iii) a ranking of friends according to their privacy attitude; and (iv) the frequency of communication with friends. The use of a cubic bezier curve facilitates the representation of different types of users' behaviors towards privacy. The inclusion of this privacy score metric could imply a manual sorting process of friends based on the personal view of the user. The proposed score only considers an ego-user view of the social network and does not evaluate other collateral effects such as information diffusion processes in the network. Bilogrevic *et al.* [6] propose an information-sharing system that decides (semi-)automatically whether to share information with others, whenever they request it, and at what granularity. They consider a vector of 18 features to feed the classifier. The vector encodes whether the information is shared or not. Initially, users make n decisions about features to train the classifier, and then a logistic classifier makes the remaining decisions automatically predicting the users' sharing decisions. The approach requires the user intervention and also assumes that users are privacy aware of the consequences of their decisions.

Some approaches focus on providing information of users that may have received information that was not previously addressed to them. These works help users to increase

their privacy risk awareness and to define their social groups/contexts more precisely. Wang *et al.* [41] focus on the effects of soft paternalistic interventions over users' behavior on information disclosure decisions. This proposal uses three mechanisms that alert users about the risk of sharing information. The mechanisms are: (i) showing images of users that can see the information; (ii) introducing a time delay before sharing information; and (iii) showing a message if the information contains negative words. The effects of these mechanisms were analyzed over a population of 21 users. The authors payed attention to the influence over users' behaviors depending on how the privacy risk information was shown to the users. This study concludes that privacy mechanisms are good to prevent unintended disclosure. However, this mechanisms do not provide accurate information about the reachability of the information sharing action.

Other approaches use norms as a mechanism for defining the different of personal information and reasoning about this information [4]. Calikli *et al.* [8] propose an adaptive architecture that provides recommendations for sharing information and help users to re-configure user's groups. This proposal is based on two main concepts: social contexts (i.e., group membership information) and conflicts (i.e., privacy norms). Thus, this proposal requires the defintion of accurate user's social contexts and conflict rules. Kafali *et al.* [23] provide an approach based on model checking for certain properties. This system uses as input privacy agreements of the users (i.e., clauses about which relations are entitled to which privileges), user relationships, the content updated by users, as well as inference rules. The system determines whether or not a property of interest (i.e., whether OSN's commitment to hide a user's information item) can be violated in a given social network. Then, the user use this output to decide his actions. Mester *et al.* [29] presents a platform where agents interact among them to reach a consensus regarding a message to be published. Agents are aware of user's privacy concerns, expectations, and friends. When a user is about to publish new content, the agent determines which other users would be affected by the message and contacts the respective agents of those users. The negotiation protocol allow agents to discuss constraints and determines a suitable way to publish the content when none of the users' privacy is violated. In this approach, the privacy rules (i.e., privacy concerns of a user) should be predefined using a Semantic Web Rule Language. In addition, this approach is only based on direct contacts and does not consider other levels of friendship that may have access to this information through a friend re-sharing action.

A more flexible approach is presented by Yang *et al.* [45]. They present a privacy metric of user i sharing information with a neighbor j as a trade-off between user i's concerns (i.e., potential privacy risks) and incentives of sharing information with j (i.e., potential social benefits). The potential privacy risk of i is based on the re-sharing probability of an information receiver j (i.e., the ratio of the number of times that j re-shares over the number of times that j receives information from a user i) and its trust level (i.e., user i's opinion on j).

The social gain considers the receivers that belong to a selected sharing circle and the number of interactions between i and j. They present the privacy risk as an individual metric, without considering the consequences that other potential users might re-share the received information. Pensa *et al.* [51] propose a privacy metric that includes information sensitivity and the location of a user in the network structure using a centrality metric. Although they metric proposed is interesting, the authors use the page-rank metric without analyzing other centrality metrics that might fit better to the context of information diffusion and might be applied in scenarios where there is no global information of the network.

There are other works focused on the analysis of the effects of information diffusion in social networks using SIR models. Zhu *et al.* [52] define a privacy protection mechanism based on information sharing in ONS and classify users according to different privacy setting policies. They use a SIR model to describe the dynamics and evolution of information propagation. However, in this proposal the authors classify users based on a static privacy policy. They do not consider that, depending on the information, the privacy policy of a user might change. Similarly, Bioglio and Pensa [48] use a SIR model to analyze the role of attitude on privacy of a user and her friends on information propagation in OSN. They use an extension of a SIR model that considers the privacy attitude of users using parametric values [49]. In the simulations, the authors consider that all the neighbouring users of the initial user where the diffusion is going to start are going to have the same attitude as the user that starts the diffusion. This is not very realistic due to a user usually have different groups of friends with different attitudes in social networks.

From our point of view, privacy risk does not only concern the problem that information might reach people who were initially not expected to receive it. Previous works focus on this problem providing mechanisms to avoid audience misalignment. In this paper, we assume that users who received the information are in the expected target audience and we focus on the next step. Our proposal is focused on the analysis of the effects over the users' privacy when users from the intended audience re-share the original publication.

The proposal privacy metrics (Reachability and Audience) improves previous works in the following ways: (i) it focuses on information sharing behaviors instead of static user's profile configuration; (ii) it does not require previous user intervention, norms definition, or manual classification of friends; (iii) the proposed metrics does not provide a unique value to represent the risk of sharing activities; it provides the metrics considering layers of friendship (i.e., confidence) that provides a more accurate view of the disclosure effect over user's privacy.

III. PRIVACY THREATS IN OSN
Privacy risk not only concerns the problem that information might reach people who were initially not expected to receive it, but it also involves the problem of losing control over the scope of the information. Figure 1 describes this
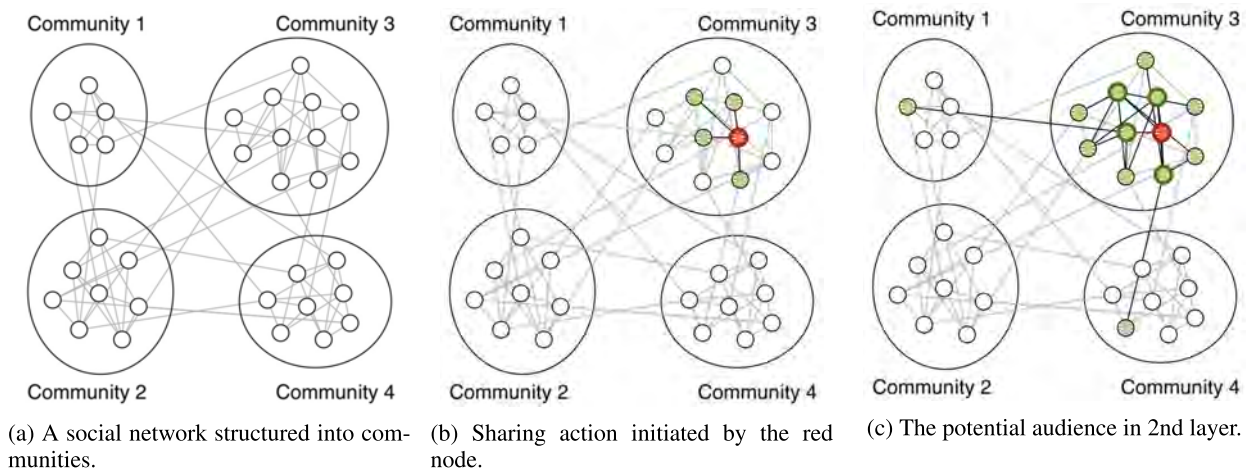
(a) A social network structured into communities.

(b) Sharing action initiated by the red node.

(c) The potential audience in 2nd layer.

FIGURE 1. Example of a potential privacy risk in online social networks.

privacy risk problem in online social networks. The elements shown have the following meaning: nodes represent users; lines represent friendship relations; scribbled-nodes represent users with content access; encircled-nodes (colored) represent users who share content.

In Figure 1a, we show the structure of a social network that is organized into four communities. Figure 1b shows the action "sharing message on his/her wall" performed by the red node. The node determines the audience depending on his selected privacy policy (e.g., *friends*). Therefore, only his friends can see the message (i.e., nodes scribbled in green). If a green node performs a sharing action (i.e., nodes encircled in green), the message could reach other communities causing a privacy risk problem (see Figure 1c, new nodes scribbled in green in community 1 and 4). The privacy risk of each node variates, as can be seen in the scenario, depending on its position in the social network and his behavior. Therefore, it is important to provide metrics about potential privacy risks to users for improving their control and awareness of the privacy.

Taking into consideration the problem described, there are a lot of moments using social media where this problem may appear. For example, there are situations where users need to use social media as therapy making negatives comments about work, politics or religion [44]. This actions can become viral (or "far-reaching", depending on user's perception) causing privacy risks and users' regret [47]. The use of social media knowing the reachability of users' publications would increase the awareness of users' actions reachability and would reduce users' privacy risk. In addition, there are many articles that analyse silent listeners or invisible audiences and the effect of their actions on users privacy [5], [37]. When users share photos about their holidays with relatives and friends, they may expect that these photos will be seen indirectly by friends of friends; but previous research studies revealed that users are only aware of a small part of the real audience that sees the publication [5].

To deal with the above privacy risk problems, we define two privacy metrics: Reachability and Audience. These metrics estimate the privacy risk of a user when shares a message in a social network. These metrics can be applied to users' friendship layers. Reachability metric obtains the probability of a message to reach a specific ratio/percentage of users given a specific sharing action. The user can specify this ratio. The Audience metric obtains the percentage of users that will see a message given a specific sharing action and a friendship layer revealing the invisible audience. These metrics aim to increase the users' awareness about the reachability of their publications in the social network even though they have restricted the visibility of their publications.

IV. PRIVACY RISK METRICS WHEN SHARING INFORMATION

To define how Reachability and Audience work, first we are going to explain some important concepts. We assume that there is a social network $\mathcal{G}$ that consists of N nodes, where every node $a_i \in N = \{a_1, ..., a_n\}$ represents a user. Users are connected through bidirectional and undirected links that represent friendship relationships and correspond to the edges $E \subseteq N \times N$ of $\mathcal{G}$. We define the adjacency matrix A to represent these links. Given two users a_i and a_j, if there is a link between these users, we represent this as $A_{a_i,a_j} = 1$ and $A_{a_i,a_j} = 0$ if there is not a link.

The privacy metrics proposed to evaluate the risk of sharing information actions (e.g., publishing a message in his/her own wall, commenting an existing post, sharing a post, etc.) act as an indicator of the potential risk of the messages diffused over the social network (i.e., potential scope and visibility). The higher the Reachability and Audience values, the higher the threat to user a_i's privacy by performing a sharing information action.

A. METRICS CALCULATION

In the social media context, users perform message diffusion actions that have a potential risk associated with the potential

subsequent action that may diffuse the message over the social network. In addition, another point to take into consideration is that not all users have the same view of risk when sharing information. Some users may consider that sharing information with ''friends of friends'' might be risky while other users may consider that the true risk is at the next layer of friendship. Moreover, some users may consider risky that few users (one or two) of a certain layer of friendship see some information while other users may consider risky only when the majority of users of a certain layer see it. In order to consider different perceptions of risk in sharing actions in social networks, we have defined the concepts of friendship layer and information reachability.

Friendship layer is based on the social distance between users. We define the distance between any pair of users a_i and a_j as the minimum number of links to be traversed to reach one a_j from a_i and is represented as $d(a_i, a_j)$.

We define a friendship layer $L_{a_i}(l)$ as the subset of users whose distance to the source user a_i is l:

$$L_{a_i}(l) \subseteq N, \quad \forall a_j \in L_{a_i}(l) : d(a_i, a_j) = l \wedge \nexists d'(a_i, a_j) < d(a_i, a_j)$$

Therefore, users in layer 1 are those that are direct neighbors of a_i, users in layer 2 are those that are linked with 2 links from a_i and so on.

We define the information reachability of a user a_i as the number of users that saw a message m published by a_i. We define a $N \times N$ reachability matrix γ_m for each message m that is diffused on the social network. The rows and the columns of γ_m represent users. We use $\gamma_m(a_i, a_j)$ to refer to the entry in the a_ith row and a_jth column of γ_m, and it has two possible values [0, 1], where 1 represents that message m was sent by a_i and reached a_j and 0 that did not reach a_j. $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$ represents the set of all γ_m associated to each messaged propagated in the network.

Based on the friendship layer and the information reachability, we define two metrics, Reachability and Audience, to provide feedback about the privacy risk of a user when shares information in a social network.

Reachability ($Re(a_i, l, r)$) represents the probability of a message diffused by a user a_i of reaching a percentage r (i.e., reachability ratio) of users in layer l. Considering $L_{a_i}(l)$ as the set of users in layer l from a user a_i and r as a reachability ratio of users, Reachability metric can be calculated as

$$Re(a_i, l, r) = \frac{|\Gamma''|}{|\Gamma'|}, \tag{1}$$

where Γ' represents the set of reachability matrixes associated to messages in which a_i participated in their diffusion, $\Gamma' \subseteq \Gamma$, such that $\forall \gamma_m \in \Gamma' \rightarrow \exists a_k |\gamma_m(a_i, a_k) = 1$; and Γ'' represents the set of reachability matrixes associated to messages in which a_i participated in the information flow and were viewed by a percentage of users of layer l greater than r

$$\Gamma'' \subseteq \Gamma', \quad \text{such that } \forall \gamma_m \in \Gamma'' \rightarrow \frac{\sum\limits_{a_j \in L_{a_i}(l)} \gamma_m(a_i, a_j)}{|L_{a_i}(l)|} \geq r$$

The Reachability metric ($Re(a_i, l, r)$) is appropriate to evaluate the risk that a message shared by a user reaches certain friendship layer. Figure 2 shows an example of Reachability metric calculation for user a_1, at friendship layer 3, and considering a ratio r of 0.15 ($Re(a_1, 3, 0.15)$). In this scenario, a_1 wants to obtain the probability that a publication in its wall will reach a few users (i.e., $r = 0.15$) at friendship level 3. The value of Re ($Re = 2/3$) means that there is a high probability (greater than 0.5) that the information reaches level 3.

Audience (Au) represents the percentage of users in layer l that is expected to see a message diffused by a_i considering the total number of users of that layer $Au(a_i, l)$ (Eq. 2), or considering the total number of users of the network $Au_G(a_i, l)$ (Eq. 3). The audience $Au(a_i, l)$ provides a local insight about the risk in a specific layer of the social network. However, the information that $Au(a_i, l)$ provides about the audience that has seen a message in a specific layer could be biased by the number of agents in that layer. Therefore, it could be also interesting for the user to obtain a more global picture of the risk of reaching certain layer considering the whole network. For this reason, we have also proposed the $Au_G(a_i, l)$ metric considering the total of agents of the network.

$$Au(a_i, l) = \frac{\sum\limits_{\gamma_m \in \Gamma'} \left(\frac{\sum\limits_{a_j \in L_{a_i}(l)} \gamma_m(a_i, a_j)}{|L_{a_i}(l)|} \right)}{|\Gamma'|} \tag{2}$$

$$Au_G(a_i, l) = \frac{\sum\limits_{\gamma_m \in \Gamma'} \left(\frac{\sum\limits_{a_j \in L_{a_i}(l)} \gamma_m(a_i, a_j)}{|N|} \right)}{|\Gamma'|} \tag{3}$$

The Audience metrics are appropriate to evaluate the privacy risk of a sharing action based on the coverage that this action will achieve at certain friendship layer. Figure 2 shows the calculation of the Audience metrics for messages sent by user a_1 considering the third level of friendship. In this scenario, a_1 wants to know exactly the percentage of users (i.e., the audience) that will see a publication on his wall. Therefore, a_1 will consider the audience metrics.

Figure 2 shows a scenario that represents an example of a social network with interactions between users. In the scenario, there are three friendship layers and the reachability matrix associated with each message generated in the social network (i.e., γ_1, γ_2, and γ_3). We assume that all of the users in $\mathcal{G}$ have the privacy policy that only their direct friends can see their walls. The message diffusion actions performed in this scenario are the following. In Case 1 (1), user a_1 publishes a message m_1 on his/her wall. Therefore, users a_2 and a_3 can see the message m_1. The information about the users that see m_1 as a result of this sharing action performed by a_1 is stored in γ_1. In γ_1, we are measuring the reachability of the m_1 when a user interacts with the message (2). Then, user a_3 decides to share m_1 on his/her wall. Users a_4, a_5, a_6, a_7, and a_8 can see the message m_1. As in the previous case, the information about the users that can see the message
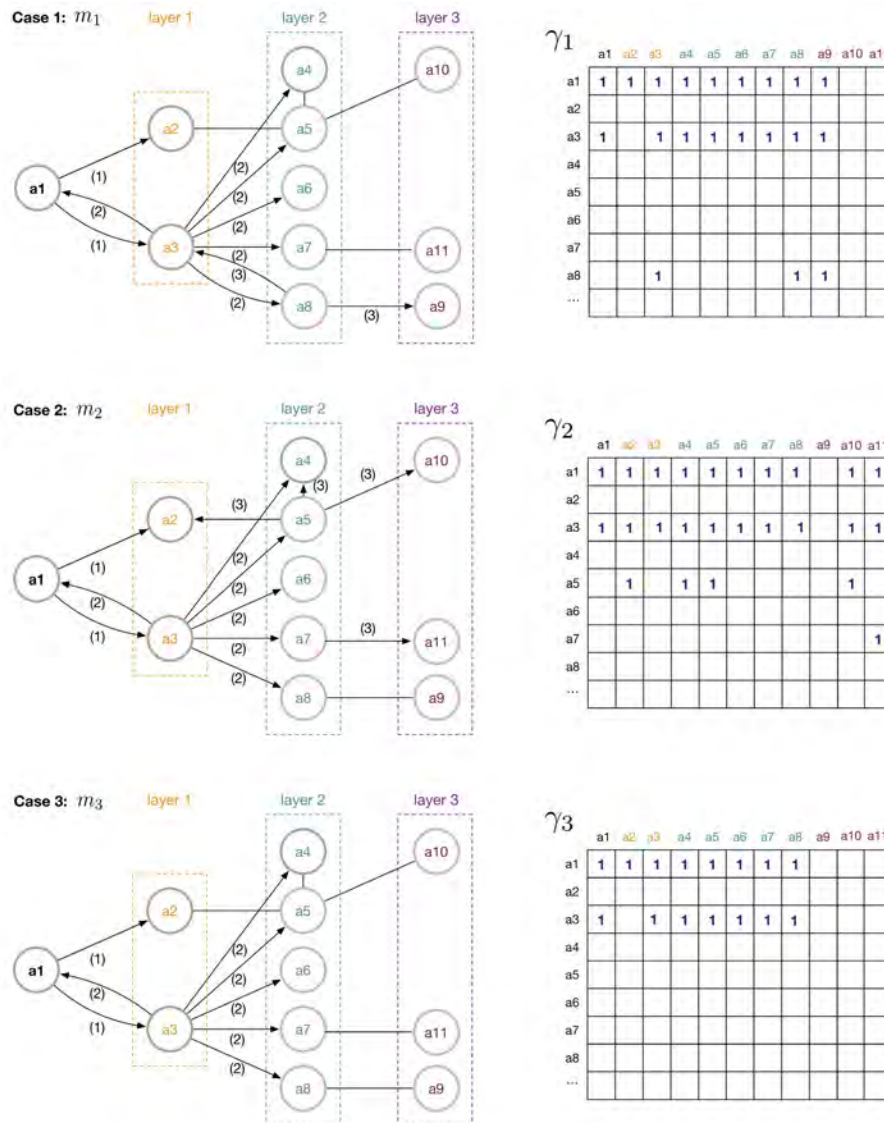
FIGURE 2. Example of social network activity and the calculation process of the Reachability and Audience metrics. In this example, all information shared is visible by users' direct friends. The directed arrows indicate the direction of the message. The number between brackets indicates the stage in the forwarding process of a message. Users perform the following actions on the social network: (case 1) user a_1 publishes/shares a message m_1 on his/her wall and users a_3 and a_8 re-share m_1; (case 2) user a_1 publishes/shares a message m_2 on his/her wall and users a_5 and a_7 re-share m_2; (case 3) user a_1 publishes/shares a message m_3 on his/her wall and users a_3 re-shares m_3.

m_1 as a result of the sharing action of a_3 is updated in γ_1. Note that the corresponding row of a_1 is also updated with the new users that see m_1. This update reflects the 'indirect' reachability of user a_1 through the actions of a_3 (3). Then, user a_8 shares m_1 publishing it on his/her wall. Users a_3 and a_9 can see it and the information in γ_1 is updated. As in the previous situation, rows corresponding to users a_3 and a_1 are also updated. In the cases 2 and 3 (i.e., messages m_2 and m_3 respectively), the process performs in a similar way to the case 1. The difference is that the users that re-share the message are different. In the case 2, the users that re-share the m_2 are a_3, a_5 and a_7. In the case 3, the user that re-shares

the m_3 is a_3. The corresponding reachability matrixes (i.e., γ_2 and γ_3) are updated accordingly to the sharing actions performed by the users. Following the example, the metric values of Reachability and Audience proposed in this paper of the user a_1 for a three-level depth and a 15% correspond to 0.66 (Re), 0.33 (Au), and 0.09 (Au_G) respectively. A Reachability value of 0.66 means in this case that 2 out of 3 times the message reached more than 15% of the users at third-level depth. An Audience value of 0.33 means in this case that as average 1 out of 3 users on the third-level will have access to the message, that at the same time corresponds to a 10% of the users on the whole network (0.09).

TABLE 1. Networks structural properties.

Model	Watts-Strogatz	Barabási-Albert	Erdös-Rényi
type	small-world	scale-free	random
# agents	1000	1000	1000
mean degree	12	12	12
diameter	5	5	5

V. EXPERIMENTS

Several experiments were performed to evaluate the privacy risk metrics proposed: Reachability and Audience. There are two sets of experiments. The first set evaluates the privacy risk metrics in different network topologies considering different layers. The second set of experiments analyzes if there is a correlation between the privacy metrics proposed and structural properties of the networks. The use of structural metrics would facilitate the estimation of the privacy metrics proposed in scenarios where there is no data available about users' information flows.

For both set of experiments, we use a social network simulation tool. This simulation tool was developed using the open source Elgg framework [1] where is possible to build real and virtual social environments. The simulation tool is capable of reproducing social network scenarios such as the creation of users and relationships, message sending, and social interactions.

A. EXPERIMENT SETTINGS

The networks generated in the experiments follow three models: Watts-Strogatz [42] (WS, small-world), Barabási-Albert [3] (BA, scale-free), and Erdös-Rényi [12] (ER, random). Table 1 shows the set of parameters and properties that characterize each of the networks used for the simulations.

Each simulation run consists of 1000 seed messages published by randomly selected agents. These seed messages cause that other agents, in turn, perform actions to diffuse the messages throughout the network. The diffusion of a message m occurs when an agent a_i sees a publication. Then, the agent evaluates the risk of sharing m considering the reachability or the audience metrics (Re, Au or Au_G depending on the scenario) values. If the value of the corresponding metric is greater than his individual risk threshold (i.e., a random uniform distributed value in the range [0,1]), a_i does not perform the action, simulating that the agent decided not to propagate the publication. Otherwise, a_i shares the message m. In the latter case, the message could be seen by other neighbor agents and the matrix γ_i will be updated. Figure 3 summarizes the specific diffusion model adopted in the simulation which corresponds to a combination of a SIR model with a threshold value.

We perform 50 simulations per each type of network and considering friendship layers $l = 2$, $l = 3$ and $l = 4$ (see Table 2). For Reachability metric (Eq. 1), we considered two reachability ratio values: $r = all$, where the label *all*

[1]https://elgg.org/
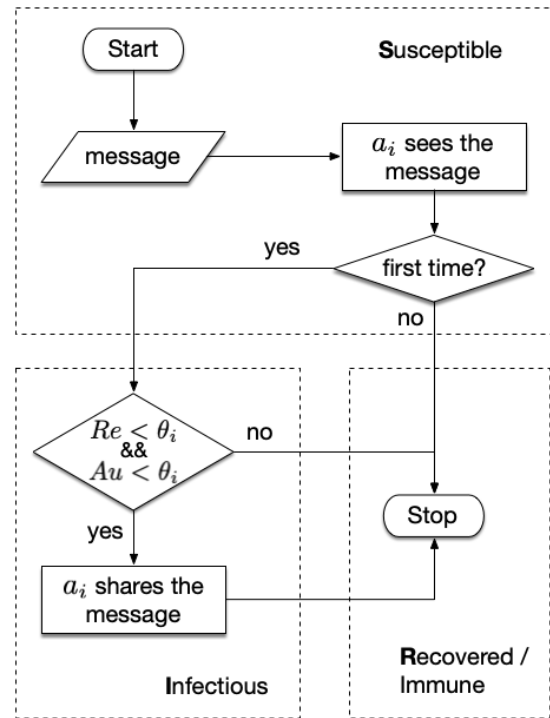
FIGURE 3. Flowchart of the diffusion model followed for each agent in the simulation.

TABLE 2. Experiment settings.

Parameter	Values
network models	Watts-Strogatz, Barabási-Albert, Erdös-Rényi
# agents	1000
privacy policy	friends
layers	2-4
# simulations per network	50
# seed messages per simulation	1000

represents the ratio percentage of 100% in the specified layer (i.e., if the message reaches all the agents of the layer); and $r = one$, where the label *one* represents the ratio percentage to reach one agent in the specified layer. This percentage value will change in each agent since the total number of agents in a layer is not equal for all the agents. For Audience metrics (Eq. 2 and 3), we consider the population of a specific layer Au and the whole population of the network Au_G.

B. PRIVACY METRICS IN DIFFERENT NETWORK TOPOLOGIES

In this section, we analyze the performance of the Reachability and Audience metrics in the three network topologies considered. Tables 3 and 4 summarize the results of the simulations.

As it can be observed in Table 3, the value of Re for $r = all$ is 0 or a value close to 0 for layers 2-4 in all the networks

TABLE 3. Statistical analysis of Reachability (*Re*) values for different network topologies (*mean ± std*).

mean ± std	small-world	scale-free	random
$Re(a_i, 2, one)$	.514 ± .121	.514 ± .121	.606 ± .025
$Re(a_i, 3, one)$	.901 ± .054	.765 ± .113	.950 ± .045
$Re(a_i, 4, one)$	.945 ± .038	.784 ± .151	.968 ± .048
$Re(a_i, \{2,3,4\}, all)$	0.0	0.0	0.0

TABLE 4. Statistical analysis of Audience (*Au*) values for different network topologies (*mean ± std*).

mean ± std	small-world	scale-free	random
$Au(a_i, 2)$	22.56 ± 1.28	13.24 ± 4.37	18.56 ± 0.98
$Au(a_i, 3)$	24.48 ± 2.99	28.77 ± 3.40	42.73 ± 5.37
$Au(a_i, 4)$	39.13 ± 5.36	40.91 ± 9.31	70.51 ± 5.95
$Au_G(a_i, 2)$	2.51 ± 0.57	2.09 ± 1.94	3.66 ± 0.96
$Au_G(a_i, 3)$	14.73 ± 2.87	19.60 ± 3.13	31.24 ± 3.71
$Au_G(a_i, 4)$	10.61 ± 1.59	5.23 ± 3.78	3.63 ± 2.53

structures. These results show that it is difficult that a message reaches all the agents in the network. However, the value of *Re* for $r = one$ increases as the layer increases in the three network structures. Initially, according to the privacy settings of the agents in the network, all direct friends of an agent a_i (i.e., agents in layer $l = 1$) see the publication of a_i. Therefore, the *Re* in that layer is 1. Then, a subset of these direct friends will re-share the publication. As a result, among all the possible agents at layer 2, only those that are direct contacts of the subset agents that re-shared will see the publication. For this reason, the probability to reach an agent in layer 2 (i.e., $Re(a_i, 2, one)$) decreases to 0.5. In the following layers the *Re* value increases considerable. The main reason for this is that the publication has been widely propagated in the network and there is a high probability that agents in layers 3 or 4 receive the same publication from different sources (i.e., agents). The values of *Re* are higher in small-world and random networks due to there is a higher degree of clustering in these topologies than in scale-free networks. Therefore, there is a higher probability that an agent receives the same information from different sources.

The *Re* metric for $r = one$ captures the idea of the reachability that a publication can achieve in a specific layer. However, this information can be completed with the consideration of the audience in a specific layer. In order to know the percentage of agents that see a message in a specific layer, we calculate the values of Audience for the agents (see Table 4). The results obtained with *Au* show a similar trend to the results obtained with *Re*. The percentage of agents that see the message increases as the layer increases in the three network structures. The highest values of *Au* are obtained by agents in random networks.

The audience that has seen a message in a specific layer could be biased by the number of agents in that layer. Therefore, we have also analyzed the Au_G metric considering the total of agents of the network. As in the case of *Au*, the highest values of Au_G are obtained in random networks. In the case of Au_G metric, there is a difference with respect the trend in the values obtained with *Au* and *Re* when a message arrives at layer $l = 4$. In the scenario that we have considered for the experiments, the networks have a diameter of 5. When a message arrives at a layer close to the diameter, the number of agents in that layer is usually low. It is very likely that there is an alternative shorter path to the agent that originated the message. Therefore, the number of agents in that layer is low with respect to the total of agents in the network and the values of Au_G are also low.

Taking into account the results of Reachability and Audience obtained in the experiments, we can conclude that the network topology has a direct effect on the outreach of the information published and therefore, in the proposed metrics. Results also show that there is a high probability that in a scenario where the agents' privacy policy is "friends", a publication reaches a layer $l = 3$, and inside this layer, in the case of random networks, the percentage of agents that could see the publication could arrive close to 30% of the network. The results obtained with Reachability and Audience metrics reinforce the theories of invisible audiences [5].

In spite of the Reachability and the Audience estimations provide a suitable measurement of the privacy risk associated with a user's publication action, the calculation of these values presents limitations under certain situations. In real-world scenarios, it is not always computationally affordable the collection and analysis of a detailed record of the sharing activity in an OSN. This becomes more complicated if the OSN frequently modifies its structure. Moreover, the access to users' information and their activities in some OSN applications to third-party applications is not always possible. It can also happen that even if we have access to the activity of users, there are situations (e.g., when a new user joins the social network) where we do not have information about the previous activity of users. For these reasons, in the following sections, we propose an approximation that evaluates the use of structural network properties to estimate Reachability and Audience metrics. Specifically, considering the previous results, we have selected the $Re(a_i, l, r = one)$ and Au_G metrics for the following analysis.

C. CORRELATION BETWEEN PRIVACY METRICS AND STRUCTURAL PROPERTIES

In this section, we present an approximation based on structural network metrics. This approximation does not use information about the traces of the paths follows by users' messages in OSN. We analyzed the relationship between the Reachability and the Audience of a user and his centrality values.

1) GLOBAL STRUCTURAL CENTRALITY PROPERTIES

Initially, we considered global centrality metrics to evaluate if there is a relationship between the privacy risk metrics and centrality. These centrality metrics use information about
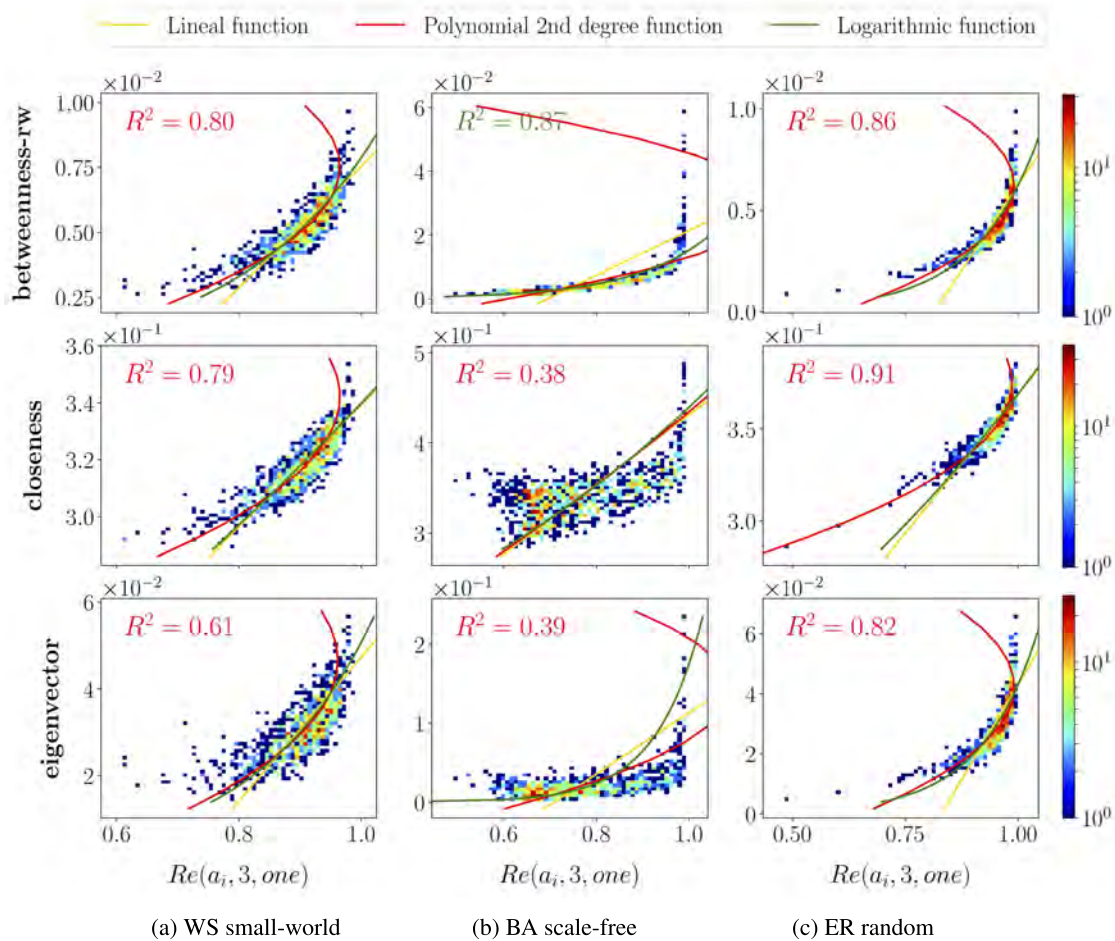
FIGURE 4. Approximation of *Reachability* metric at layer *l* = 3 using global centrality metrics (different network topologies considered).

TABLE 5. Dependence strength between global centrality properties and privacy risk (*Reachability* and *Audience*) values measured using the R^2 coefficient. The best adjustments have been highlighted. Header columns correspond with random-walk betweenness centrality (RW_BC), closeness centrality (CC), and eigenvector centrality (EC).

R^2	*small-world*			*scale-free*			*random*		
	RW_BC	CC	EC	RW_BC	CC	EC	RW_BC	CC	EC
$Re(a_i, 2, one)$	**0.69**	0.48	0.34	**0.85**	0.25	0.24	**0.73**	0.50	0.43
$Re(a_i, 3, one)$	**0.80**	**0.79**	0.61	**0.87**	0.38	0.39	0.86	**0.91**	0.82
$Re(a_i, 4, one)$	**0.55**	0.51	0.52	**0.67**	0.24	0.34	**0.49**	0.48	0.49
$Au_G(a_i, 2)$	0.81	**0.92**	0.75	**0.97**	0.92	0.90	0.90	**0.96**	0.95
$Au_G(a_i, 3)$	0.71	**0.93**	0.72	0.20	**0.82**	0.34	0.49	**0.56**	0.54
$Au_G(a_i, 4)$	0.53	**0.81**	0.61	0.21	**0.96**	0.83	0.80	**0.96**	0.94

the entire network structure to be computed. Among the global metrics, we have considered [31]: (*i*) random-walk betweenness [32] that considers the number of times a random walk between two pairs passes through the agent of interest; (*ii*) closeness, that considers the average length of the shortest paths between an agent and all other agents in the network; and (*iii*) eigenvector, that gives each agent a score proportional to the sum of the scores of his neighbors. The values of the centrality metrics were normalized in [0, 1] interval.

Using analytical regression, we study how each centrality metric is related to the values of Reachability and Audience. For this, we performed regression tests where a regressor is launched for each centrality metric. Figures 4 and 5 show the relationship between Reachability (or Audience) and centrality values. The point color represents the number of agents with specific values of the metrics. We considered the R^2 coefficient to determine how close the values of the metrics are to the regression model. R^2 values close to 1 indicate that there is a high correlation between Reachability
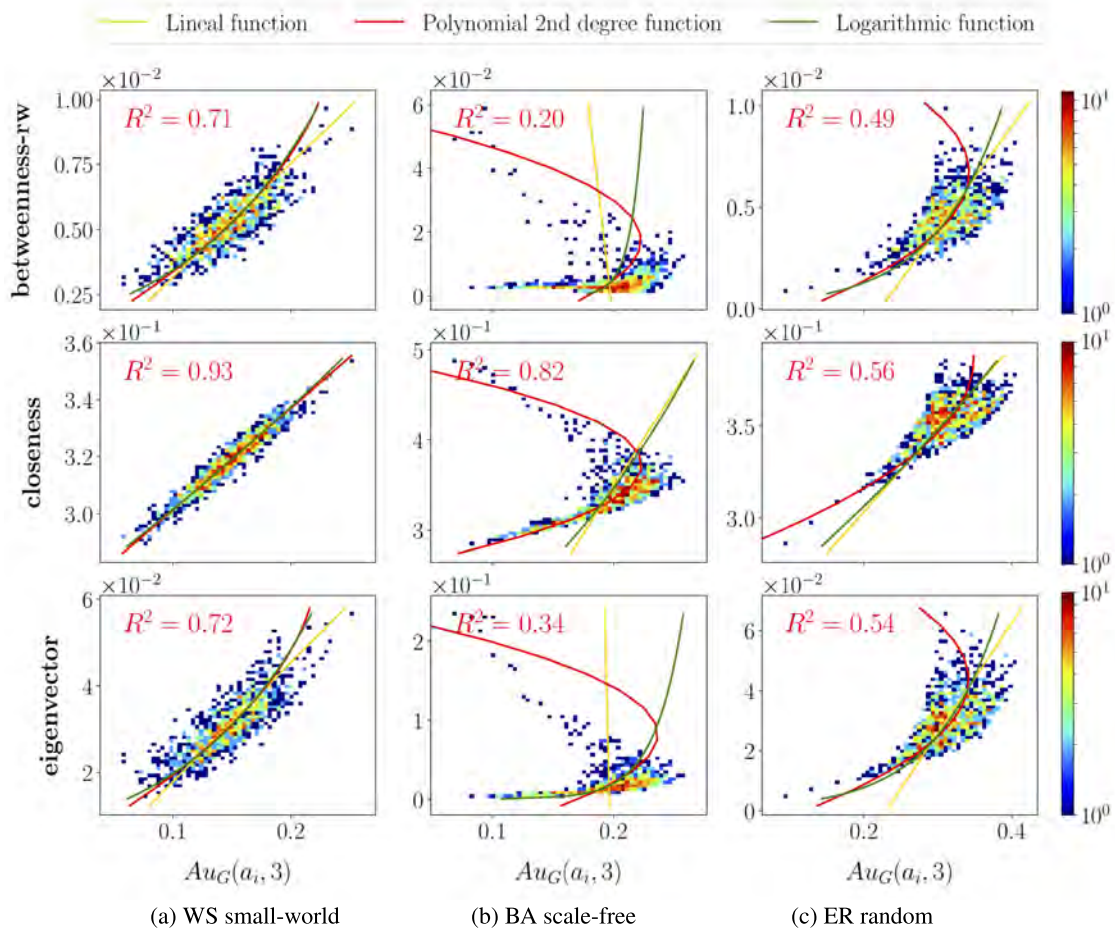
FIGURE 5. Approximation of *Audience* metric at layer *l* = 3 using global centrality metrics (different network topologies considered).

(or Audience) and the centrality metric. The regression models considered in the experiments are linear, polynomial and logarithmic.

First, we analyze the accuracy of global centrality measures to estimate the Reachability metric by layers (see Table 5). In general, independently of the layer and the network topology, the best results are obtained by the random-walk betweenness centrality. Figure 4 shows the relationship between the Re at layer 3 and global centrality metrics in each network topology considered. We can observe that the polynomial regressor model has slightly higher R^2 values than the linear or the logarithmic. The polynomial regressor model allows adjusting to a linear correlation, especially in the case of the small-world network, whereas in the scale-free network and in some cases the random network its behaviour tends to be curved and therefore it improves remarkably to other adjustments.

Second, we analyze the accuracy of global centrality measures to estimate the Audience metric by layers (see Table 5). The R^2 coefficient values show that there is a clear relation between closeness centrality and the Au_G metric. Figure 5 shows the relationship between the Au_G metric at layer 3 and global centrality metrics in each network topology.

The polynomial regressor model provides the best R^2 coefficient values, especially in the case of the small-world network. In the scale-free networks, the correlation values between the global centrality metrics and the Au_G are low, except for closeness centrality metric. It can also observed that for agents with high centrality values, their Au_G values are low. The main reason for these results is that in scale-free topologies, when the Au_G is calculated for layers close to the network diameter (d = 5), the number of agents that have not been received the message yet is low compared to the total number of agents in the network.

Considering the global centrality measures analyzed, random-walk betweenness metric provides a more fitted approximation to Reachability metric, while closeness metric provides a more fitted approximation to Audience metric.

Another phenomenon that can be observed is the distribution of agents in different groups depending on network topology and the metrics. In Figure 4, we observe that most of the agents in small-world networks have high Re values (values close to 0.9) compared to other network topologies, and there are two extreme minorities: one with lower Re values ([0.6, 0.85]) and another with slightly higher Re values ([0.9, 1]). In the scale-free networks, there is a small group
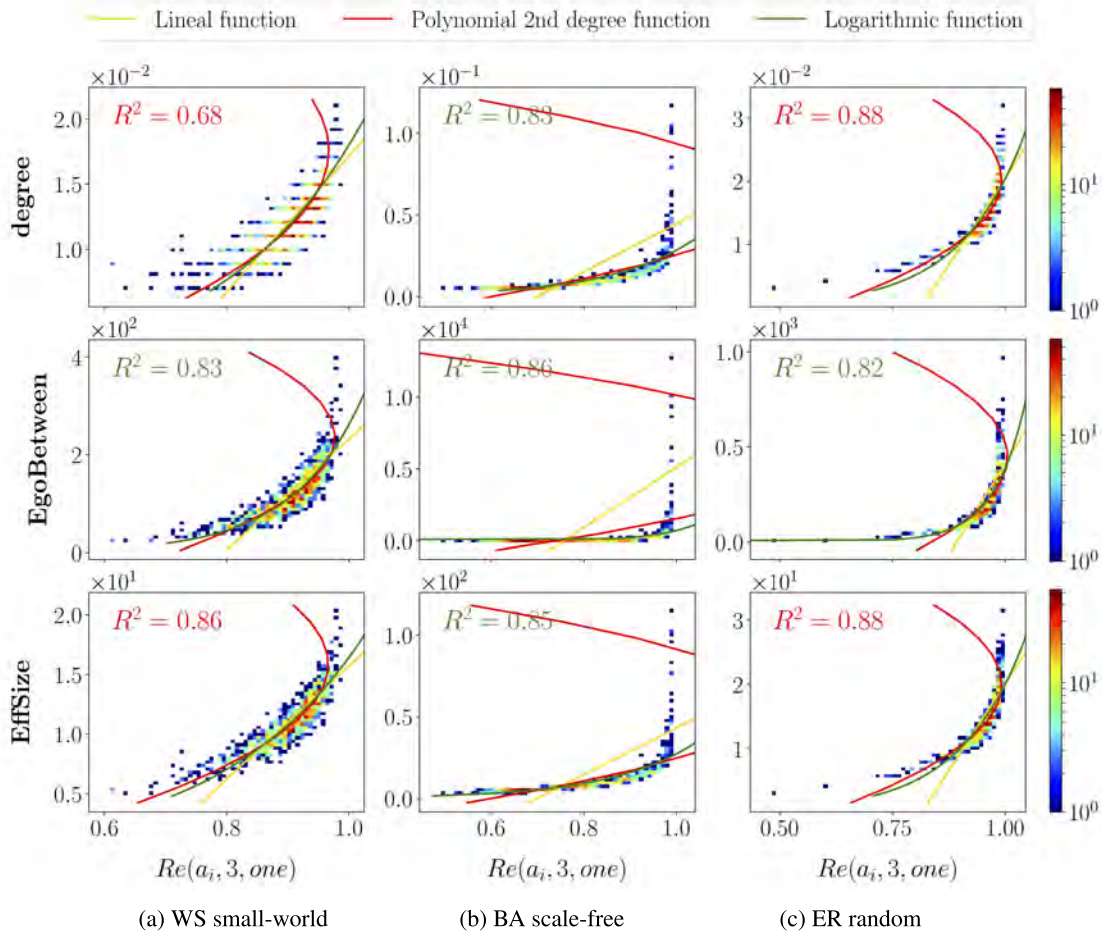
FIGURE 6. *Approximation* of *Reachability* metric at layer *l* = 3 using local centrality metrics (different network topologies considered).

of agents with high values of *Re* metric ([0.8, 1]) while the rest of agents are distributed between 0.6 and 0.8 values of *Re*. In the random networks, there is a core group with high values (between 0.9 and 1) and a minority of agents with values of *Re* between 0.7 and 0.9. Therefore, in this scenario, the topologies where there is a large group of agents with a high degree of Reachability are random and small world networks.

Something similar occurs in Figure 5. In the small-world network for layer *l* = 3, we observe that most of the agents have intermediate Au_G values (i.e., values close to 0.15) compared to other network topologies, and there are two extreme minorities: one with slightly lower Au_G values ([0.1, 0.12]) and another with slightly higher Au_G values ([0.17, 0.22]). In the scale-free networks, there is a small group of agents with high values of Au_G metric ([0.15, 0.22]) while the rest of agents are distributed between 0.1 and 0.15 values of Au_G. In the random networks, there is a core group with relatively high values (0.35) and a minority of agents with very low values of Au_G. Therefore, in this scenario, the topologies where there is a large group of agents that can reach a wider audience are scale-free and random networks.

2) LOCAL STRUCTURAL CENTRALITY PROPERTIES

Global structural centrality properties are suitable for social networking services providers that have access to the network structure. Otherwise, some OSN applications do not facilitate access to users' information to third-party applications, therefore it is not possible to infer the social network structure beyond the first layer. For these reasons, we have also considered strictly local metrics to evaluate their suitability to estimate Reachability and Audience values in layers.

Considering the limitations to calculate global centrality metrics, in this section we examine local centrality metrics. We considered degree, the number of links of an agent; ego-betweenness, an ego-centric method to approximate the betweenness centrality; and effectiveness, an ego-centric method that measures the number of alters minus the average degree of alters within the ego network, not counting ties to ego network [1]. The effectiveness reflects the links that lead to different people. A high value of effectiveness implies that the agent can lead to a high number of different people.

Table 6 shows the results of the analysis of the relation between Reachability and local centrality metrics in different network topologies. It can be observed that the best results are obtained with the effectiveness centrality. Figure 6 shows

TABLE 6. Dependence strength between local centrality properties and privacy risk (*Reachability* and *Audience*) values measured using the R^2 coefficient. The best adjustments have been highlighted. Header columns correspond with degree centrality (DC), ego betweenness centrality (EGO_BC), and effectiveness (EF).

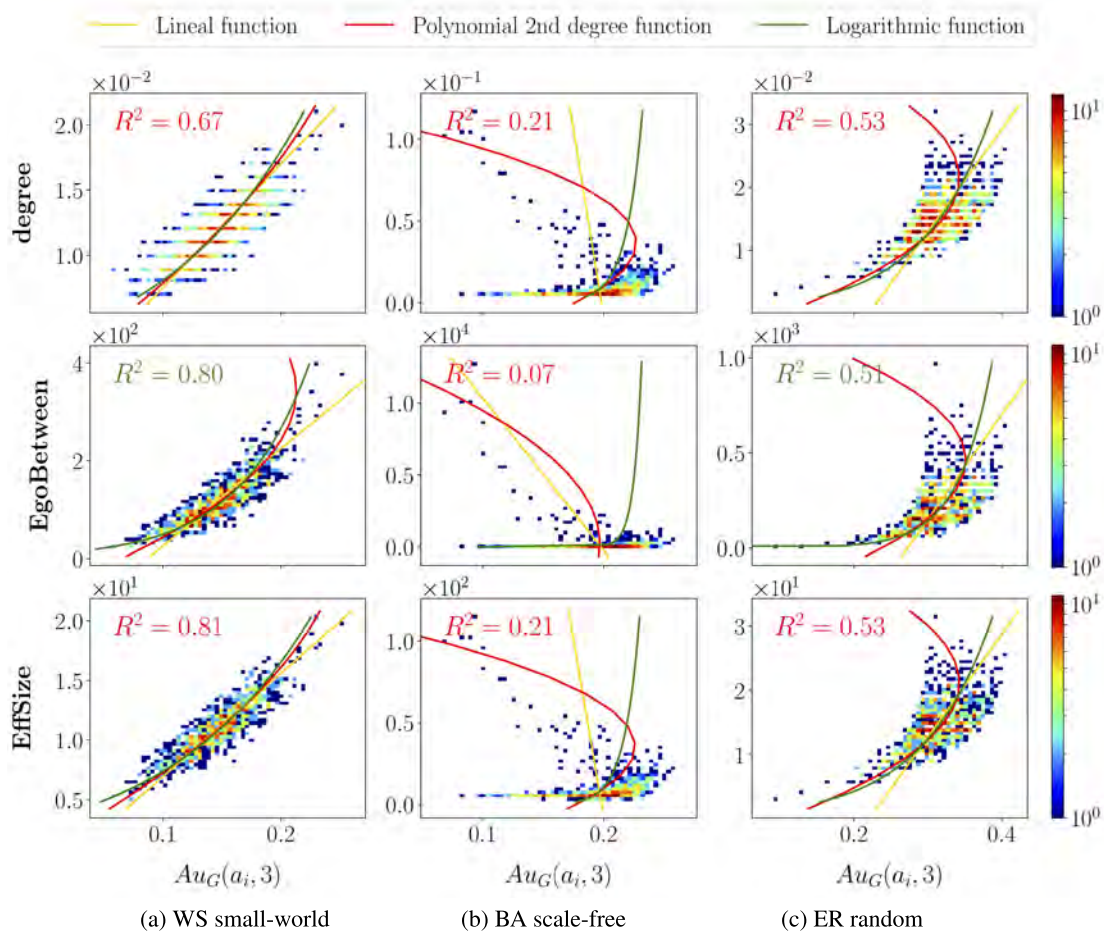| R^2 | small-world | | | scale-free | | | random | | |
	D	EGO_BC	EF	D	EGO_BC	EF	D	EGO_BC	EF
$Re(a_i, 2, one)$	0.46	0.58	**0.68**	0.72	0.78	**0.78**	0.65	0.65	**0.65**
$Re(a_i, 3, one)$	0.67	0.83	**0.86**	0.83	**0.86**	0.85	0.88	0.82	**0.88**
$Re(a_i, 4, one)$	**0.57**	0.53	**0.56**	0.69	0.43	**0.74**	0.50	0.41	**0.53**
$Au_G(a_i, 2)$	0.76	0.89	**0.90**	0.98	0.95	**0.98**	0.96	0.95	**0.96**
$Au_G(a_i, 3)$	0.67	0.79	**0.81**	0.21	0.07	**0.21**	0.53	0.51	**0.53**
$Au_G(a_i, 4)$	0.55	0.60	**0.61**	**0.28**	0.25	0.23	0.85	0.79	**0.88**

FIGURE 7. Approximation of *Audience* metric at layer *l* = 3 using local centrality metrics (different network topologies considered).

the relation between *Re* values and local centrality values for layer 3. In small-world networks, ego-betweenness and effectiveness centrality metrics yield good results, in some cases even better than global centrality metrics. In scale-free networks, the relation between *Re* and local centrality metrics is better than with global metrics. Moreover, we can observe a logarithmic relation between *Re* and local centrality values, especially in scale-free networks. In random networks, there are no significant differences between global and local metrics and their relation to the *Re* metric.

Regarding the Audience metric, Table 6 shows the results of the analysis of the relation between Audience and local centrality metrics in different network topologies. It can be observed that the best R^2 values for small-world and random network topologies are obtained using the effectiveness centrality. In the case of scale-free network topologies, there is only a high correlation values between Au_G and local centrality values for layer 2. Figure 7 shows the relation between Audience values and local centrality values for layer 3. Ego-betweenness and effectiveness centrality metrics yield

good results using a linear regressor. In scale-free networks, the relation between Audience and local metrics is similar to global metrics. We also observe a polynomial behavior between Audience and local centrality values. In random networks, there are no significant differences between global and local metrics and their relation to the Audience metric.

Results show that local centrality metrics offer similar results to global metrics to estimate Reachability and Audience values. Effectiveness centrality metric provides a slightly higher fitted approximation using the logarithmic regressor model. Results obtained with Effectiveness along with the ease of its calculation allow us to make an estimation of the proposed risk metrics (i.e., Reachability and Audience) that will assess the user in the publication process of an information item in an OSN.

If we observe the relation between the different values of privacy risk metrics and the centrality measures (global and local), we reach the following conclusions. Regarding the global centrality metrics, closeness metric has a higher correlation with privacy risk metrics, especially with Audience, in different network topologies than other global centrality metrics. In the case of Reachability, random-walk betweenness provides a higher degree of correlation. Regarding local centrality metrics, effectiveness metric achieves the best results both in the different network topologies and for the different types of privacy risk metrics (i.e., Reachability and Audience). Specifically, effectiveness metric yields promising results comparable to global centrality measures and close to the proposed privacy risk metrics (i.e., Reachability and Audience). Moreover, effectiveness facilitates the estimation of privacy risk in scenarios where there is no global knowledge or there is no previous information about users' privacy policies or information flows. Effectiveness offers a powerful advantage to provide real-time personalized solutions to users when they post or share information through ONS.

VI. CONCLUSION

In this paper, we have presented a new model of privacy risk based on friendship layers. The concept of friendship layers allows us to provide information about user's privacy risk for different levels of risk perception. Based on this model, we propose two privacy risk metrics Reachability and Audience. Reachability provides information to the user about the probability that a message that he publishes reaches a specific friendship layer or a specific number of users in that layer. Audience provides information to the user about the percentage of users in a specific layer that is probable that see a message he published.

We evaluated the proposed Reachability and Audience through simulations in different social network topologies and considering different layers. The results show that network topology has a direct effect on the outreach of the information published when agents' privacy policy is "friends". In the scenario analyzed, if an agent publishes a message, there is a high probability (close to 0.9) that reaches

a layer $l = 3$ and the percentage of agents that could see the publication will be close to 30% of the network. The results of the simulations provide a real vision of the privacy risk that is higher than the users risk initially might think, which reinforces the theories of invisible audiences.

Finally, we consider a different approximation of Reachability and Audience for scenarios where there is no previous information about users activity or the information about the traces of the messages cannot be obtained. The proposed approximations are based on structural centrality metrics. We analyzed the relation between Reachability and Audience and centrality metrics. We considered global centrality metrics that have a complete overview of the structure of the network and the local centrality metrics that only consider local information. Regarding the global centrality metrics, the results show that, to estimate the Reachability metric the best results are obtained by the random-walk betweenness centrality. To estimate the Audience metric the best results are obtained by the closeness centrality. Regarding local centrality metrics, effectiveness is the most suitable property to approximate Reachability. In the case of the relation between Reachability and centrality metrics, there are no relevant differences between the degree of correlation values obtained with global or local metrics. To estimate the Audience using local centrality metrics, in small-world and random networks, the best results are obtained with effectiveness centrality. For scale-free networks, effectiveness provides good results for the estimation of Audience in layers that are not close to the network diameter. Based on these results, we propose a common regression model based on the effectiveness centrality values of agents to approximate Reachability and Audience values in different network models.

As future work, we plan to validate Reachability and Audience metrics in a real scenario that allows us to obtain users' feedback to evaluate the suitability of the proposed metrics. We also plan the analysis of the effects of different informative methods to show the users' privacy risk in an online social network. Finally, we will extend the proposed metrics with the inclusion of new factors about the users (such as personality and trust) and about the publication (such as sensitivity and virality). These factors may have a great influence on the diffusion of a message in the social network and provide a more precise approximation about the publications' scope.

REFERENCES

[1] A. Abbasi, K. S. K. Chung, and L. Hossain, "Egocentric analysis of co-authorship network structure, position and performance," *Inf. Process. Manage.*, vol. 48, no. 4, pp. 671–679, Jul. 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0306457311000975

[2] Y. Altshuler, Y. Elovici, A. B. Cremers, N. Aharony, and A. Pentland, *Security and Privacy in Social Networks*. Cham, Switzerland: Springer, 2012.

[3] A. L. Barabási and R. Albert "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, Oct. 1999.

[4] A. Barth, A. Datta, J. C. Mitchell, and H. Nissenbaum, "Privacy and contextual integrity: Framework and applications," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2006, p. 15.

[5] M. S. Bernstein, E. Bakshy, M. Burke, and B. Karrer, "Quantifying the invisible audience in social networks," in *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, New York, NY, USA, Apr./May 2013, pp. 21–30. doi: 10.1145/2470654.2470658.

[6] I. Bilogrevic, K. Huguenin, B. Agir, M. Jadliwala, and J. P. Hubaux, "Adaptive information-sharing for privacy-aware mobile social networks," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput.*, Sep. 2013, pp. 657–666.

[7] P. Bonacich, "Power and centrality: A family of measures," *Amer. J. Sociol.*, vol. 92, no. 2, pp. 1170–1182, 1987.

[8] G. Calikli, M. Law, A. K. Bandara, A. Russo, L. Dickens, B. A. Price, A. Stuart, M. Levine, and B. Nuseibeh, "Privacy dynamics: Learning privacy norms for social software," in *Proc. 11th Int. Symp. Softw. Eng. Adapt. Self-Manag. Syst.*, May 2016, pp. 47–56.

[9] E. Christofides, A. Muise, and S. Desmarais, "Hey mom, what's on your facebook? Comparing Facebook disclosure and privacy in adolescents and adults," *Social Psychol. Personality Sci.*, vol. 3, no. 1, pp. 48–54, Jan. 2012.

[10] G. Cluley. (2010). *60% of Facebook Users Consider Quitting Over Privacy*. Accessed: Sep. 20, 2018. [Online]. Available: https://nakedsecurity.sophos.com/2010/05/19/60-facebook-users-quitting-privacy/

[11] *Social Networks—Statista Dossier: Facts and Statistics About Social Networks*, eMarketer, New York, NY, USA, 2015.

[12] P. Erdös "Graph theory and probability," *Can. J. Math.*, vol. 11, no. 11, pp. 34–38, 1959.

[13] Eurostat. (2014). *Information Society Statistics—Households and Individuals*. Accessed: May 19, 2018. [Online]. Available: http://ec.europa.eu/eurostat/statistics-explained/index.php/Information_society_statistics_-_households_and_individuals

[14] L. Fang and K. LeFevre, "Privacy wizards for social networking sites," in *Proc. 19th Int. Conf. World Wide Web*, Apr. 2010, pp. 351–360.

[15] J. Fogel and E. Nehmad, "Internet social network communities: Risk taking, trust, and privacy concerns," *Comput. Hum. Behav.*, vol. 25, no. 1, pp. 153–160, Jan. 2009.

[16] L. C. Freeman, "A set of measures of centrality based on betweenness," *Sociometry*, vol. 40, no. 1, pp. 35–41, Mar. 1977.

[17] L. C. Freeman, S. P. Borgatti, and D. R. White, "Centrality in valued graphs: A measure of betweenness based on network flow," *Social Netw.*, vol. 13, no. 2, pp. 141–154, Jun. 1991.

[18] L. C. Freeman, "Centrality in social networks: Conceptual clarification," *Social Netw.*, vol. 1, no. 3, pp. 215–239, 1978.

[19] S. Goel, D. J. Watts, and D. G. Goldstein, "The structure of online diffusion networks," in *Proc. 13th ACM Conf. Electron. Commerce*, Jun. 2012, pp. 623–638.

[20] E. Hargittai, "Facebook privacy settings: Who cares?" *First Monday*, vol. 15, no. 8, Jul. 2010.

[21] P. R. H. Seybert. (2013). *Statistics in Focus 29/2013*. Accessed: Nov. 14, 2018. [Online]. Available: http://ec.europa.eu/eurostat/statistics-explained/index.php/Archive:Internet_use_statistics_-_individuals

[22] M. M. Joe and D. B. Ramakrishnan, "A survey of various security issues in online social networks," *Int. J. Comput. Netw. Appl.*, vol. 1, no. 1, pp. 11–14, Nov. 2014.

[23] Ö. Kafali, A. Günay, and P. Yolum "PROTOSS: A run time tool for detecting privacy violations in online social networks," in *Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining*, Aug. 2012, pp. 429–433.

[24] D. Kempe, J. Kleinberg, and É. Tardos, "Maximizing the spread of influence through a social network," in *Proc. 9th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Aug. 2003, pp. 137–146.

[25] G. Lawyer, "Understanding the influence of all nodes in a network," *Sci. Rep.*, vol. 5, Mar. 2015, Art. no. 8665.

[26] Q. Li, T. Zhou, L. Lü, and D. Chen, "Identifying influential spreaders by weighted leaderrank," *Phys. A, Stat. Mech. Appl.*, vol. 404, pp. 47–55, Jun. 2014.

[27] J.-G. Liu, J.-H. Lin, Q. Guo, and T. Zhou, "Locating influential nodes via dynamics-sensitive centrality," *Sci. Rep.*, vol. 6, Feb. 2016, Art. no. 21380.

[28] L. Lü, Y. C. Zhang, C. H. Yeung, and T. Zhou, "Leaders in social networks, the delicious case," *PLoS ONE*, vol. 6, no. 6, Jun. 2011, Art. no. e21202.

[29] Y. Mester, N. Kökciyan, and P. Yolum, "Negotiating privacy constraints in online social networks," in *Proc. Int. Workshop Multiagent Found. Social Comput.* Cham, Switzerland: Springer, 2015, pp. 112–129.

[30] N. L. Muscanell and R. E. Guadagno, "Make new friends or keep the old: Gender and personality differences in social networking use," *Comput. Hum. Behav.*, vol. 28, no. 1, pp. 107–112, Jan. 2012.

[31] M. Newman, *Networks: An Introduction*. Oxford, U.K.: Oxford Univ. Press, 2010.

[32] M. E. J. Newman, "A measure of betweenness centrality based on random walks," *Social Netw.*, vol. 27, no. 1, pp. 39–54, Jan. 2005.

[33] R. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," *Phys. Rev. Lett.* vol. 86, no. 14, pp. 3200–3203, Apr. 2001.

[34] S. Pei, L. Muchnik, J. S. Andrade, Jr., Z. Zheng, and H. A. Makse, "Searching for superspreaders of information in real-world social media," *Sci. Rep.*, vol. 4, Jul. 2014, Art. no. 5547.

[35] J. Staddon, D. Huffaker, L. Brown, and A. Sedley, "Are privacy concerns a turn-off?: Engagement and privacy in social networks," in *Proc. 8th Symp. Usable Privacy Secur.*, Jul. 2012, p. 10.

[36] F. Stutzman, R. Capra, and J. Thompson, "Factors mediating disclosure in social network sites," *Comput. Hum. Behav.*, vol. 27, no. 1, pp. 590–598, Jan. 2011.

[37] F. D. Stutzman, R. Gross, and A. Acquisti, "Silent listeners: The evolution of privacy and disclosure on Facebook," *J. Privacy Confidentiality*, vol. 4, no. 2, p. 2, 2013.

[38] B. Vidyalakshmi, R. K. Wong, and C.-H. Chi, "Privacy scoring of social network users as a service," in *Proc. IEEE Int. Conf. Services Comput.*, Jun./Jul. 2015, pp. 218–225.

[39] I. Wagner and E. Boiten, "Privacy risk assessment: From art to science, by metrics," 2017, *arXiv:1709.03776*. [Online]. Available: https://arxiv.org/abs/1709.03776

[40] Y. Wang, G. Norcie, S. Komanduri, A. Acquisti, P. G. Leon, and L. F. Cranor, "I regretted the minute I pressed share: A qualitative study of regrets on Facebook," in *Proc. 7th Symp. Usable Privacy Secur.*, Jul. 2011, p. 10.

[41] Y. Wang, P. G. Leon, K. Scott, X. Chen, A. Acquisti, and L. F. Cranor, "Privacy nudges for social media: An exploratory Facebook study," in *Proc. 22nd Int. Conf. World Wide Web*, May 2013, pp. 763–770.

[42] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[43] S. Wen, J. Jiang, B. Liu, Y. Xiang, and W. Zhou, "Using epidemic betweenness to measure the influence of users in complex networks," *J. Netw. Comput. Appl.*, vol. 78, pp. 288–299, Jan. 2016.

[44] W. Xie and C. Kang, "See you, see me: Teenagers' self-disclosure and regret of posting on social network site," *Comput. Hum. Behav.*, vol. 52, pp. 398–407, Nov. 2015.

[45] M. Yang, Y. Yu, A. K. Bandara, and B. Nuseibeh, "Adaptive sharing for online social networks: A trade-off between privacy risk and social benefit," in *Proc. IEEE 13th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Sep. 2014, pp. 45–52.

[46] E. Zheleva and L. Getoor, "To join or not to join: The illusion of privacy in social networks with mixed public and private user profiles," in *Proc. 18th Int. Conf. World Wide Web*, Apr. 2009, pp. 531–540.

[47] L. Zhou, W. Wang, and K. Chen, "Tweet properly: Analyzing deleted tweets to understand and identify regrettable ones," in *Proc. 25th Int. Conf. World Wide Web*, Apr. 2016, pp. 603–612.

[48] L. Bioglio and R. G. Pensa, "Impact of neighbors on the privacy of individuals in online social networks," *Procedia Comput. Sci.*, vol. 108, pp. 28–37, Jan. 2017.

[49] L. Bioglio and R. G. Pensa, "Modeling the impact of privacy on information diffusion in social networks," in *Proc. Int. Workshop Complex Netw.* Cham, Switzerland: Springer, 2017, pp. 95–107.

[50] K. Liu and E. Terzi, "A framework for computing the privacy scores of users in online social networks," *ACM Trans. Knowl. Discovery Data*, vol. 5, no. 1, p. 6, Dec. 2010.

[51] R. G. Pensa, G. Di Blasi, and L. Bioglio, "Network-aware privacy risk estimation in online social networks," *Social Netw. Anal. Mining*, vol. 9, no. 1, p. 15, Dec. 2019.

[52] H. Zhu, C. Huang, and H. Li, "Information diffusion model based on privacy setting in online social networking services," *Comput. J.*, vol. 58, no. 4, pp. 536–548, Jul. 2014.

JOSE ALEMANY received the master's degree in informatics engineering from the Universitat Politècnica de València (UPV), in 2016, where he is currently pursuing the Ph.D. degree under the supervision of Dr. A. García-Fornes and supported by a Spanish FPI Grant. His current research interests include information dissemination, privacy-preserving, content analysis, and complex networks.

ELENA DEL VAL received the Ph.D. degree with European mention from the Universitat Politècnica de València (UPV), in 2013. She is currently an Assistant Professor with the Universidad de Zaragoza. She has participated in several research projects related to multiagent systems, service oriented computing, social networks, and artificial intelligence. She is currently involved in intelligent privacy assessment in the context of social networks.

ANA GARCÍA-FORNES received the B.S. degree in computer science from the Polytechnic University of Catalonia, Spain, in 1986, and the Ph.D. degree in computer science from the Universitat Politècnica de València, Spain, in 1996. She is currently a Full Professor with the Department of Information Systems and Computation, Universitat Politècnica de València. Her current research interests include real-time scheduling, real-time operating systems, real-time agent/multiagent systems, and multiagent systems platforms.

• • •

JUAN M. ALBEROLA received the Ph.D. degree, in 2013. He is currently a Researcher with the Department de Sistemes Informàtics and Computació, Universitat Politècnica de València, and with Florida Universitaria. His current research interests include agent organizations, adaptation, multiagent platforms, case-based-reasoning, and electronic markets. He is also interested in educational innovation, in which, he focuses on improving the performance of teamworks.