Information Sciences 441 (2018) 50–65

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Co-utile disclosure of private data in social networks

David Sánchez*, Josep Domingo-Ferrer, Sergio Martínez

UNESCO Chair in Data Privacy, Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, Av. Països Catalans 26, Tarragona, Catalonia E-43007, Spain

ARTICLE INFO

Article history:
Received 14 June 2017
Revised 1 January 2018
Accepted 5 February 2018
Available online 8 February 2018

Keywords:
Social networks
Data privacy
Information exchange
Co-utility

ABSTRACT

Social Networks (SNs) have become the mainstream web service by which users publish and share information. However, since much of that information is personal and sensitive, disclosing it in an uncontrolled way entails serious privacy risks. Paradoxically, most SNs assume that their users are willing to disclose sensitive data to others (even strangers) with little to no control. In this paper, we formalize the utility that rational users derive from participating in SNs, and argue that the current information exchange model is hardly sustainable from a rational viewpoint; actually, it goes against the interests of privacy-aware users. To tackle this issue, we propose several *co-utile* protocols for exchanging (sensitive) information among SN users. An interaction is said to be co-utile if the best way for a participant to increase her own utility is to help other participants increase theirs; hence, co-utile information exchange is self-enforcing and mutually beneficial for rational users. In this way, we ensure the sustainability of SNs in the long term, especially SNs with a sensitive scope (e.g., healthcare).

1. Introduction

Social Networks (SNs) have ushered in a new information sharing paradigm whereby the information published on the Internet is no longer generic or anonymous, but associated to individuals. In this respect, the Consumer Reports' 2010 State of the Net analysis [11] highlights that more than half of SN users usually share private information and, as a result, they are exposed to a number of privacy-related threats, such as spamming, phishing [45], discrimination (*e.g.*, in job application) [34] or bullying [13]. Studies have also shown that the increasing awareness of the privacy threats underlying personal data publication in SNs has negatively affected the information posting rate of SN users and that many users have shifted from posting to reading [21,36]. Privacy-aware users constitute a significant problem for the sustainability of SNs [22], because SN "free-riding" (*i.e.*, getting information about others without offering information about themselves) may result in a functional standstill where no new information is offered on the SN.

Even though the consequences of the privacy concerns of SN users may affect any network, it is especially relevant in SNs with particularly sensitive scopes. For example, in LinkedIn, users disclose their CVs and their detailed professional experience for professional networking and to attract job offers or gain professional contacts; in healthcare-oriented SNs, such as PatientsLikeMe, patients share their medical conditions and healthcare experiences because they expect to learn from others' experiences. In this kind of SNs, privacy concerns may outweigh the utility benefits of information sharing and, thus, compromise the sustainability of the network in the long run.

* Corresponding author.
E-mail addresses: david.sanchez@urv.cat (D. Sánchez), josep.domingo@urv.cat (J. Domingo-Ferrer), sergio.martinezl@urv.cat (S. Martínez).

https://doi.org/10.1016/j.ins.2018.02.010
0020-0255/

SN users face two types of privacy risks: (i) those derived from the fact that all their data are hosted by a centralized SN operator, who may exploit and/or resell their personal data for business purposes, such as identity verification, marketing or personal profiling [41]; and (ii) those caused by releasing sensitive data in an uncontrolled way to other users in the SN, who may use these data for malicious purposes (*e.g.*, phishing, blackmailing, discrimination, etc.).

The former risk can be tackled by using distributed SN architectures, which avoid relying on centralized operators. Diaspora is probably the best-known example of a decentralized SN [42], even though other systems have also been proposed in the literature [12,26]. Decentralized SNs allow users to install and manage their own personal web server that locally stores all their data (*e.g.*, photos, videos, etc.). Since users control their own data, they retain full ownership over the shared content, which is not subject to changing privacy policies or sellouts to third parties.

To mitigate the second privacy risk, in this paper we propose information exchange protocols that assist users in making informed rational decisions on what (sensitive) data they reveal to their peers in the SN. To ensure the sustainability of the SN, our protocols are grounded in the notion of *co-utility* [18,19]. Specifically, *co-utile* protocols are those in which helping other peers increase their utilities is also the best way to increase one's own utility. In those SNs where the main utility is the information the users gain from others, we envision co-utile information exchange as a *quid pro quo* interaction whereby users only disclose their sensitive data to other peers that also disclose a similar amount of their own sensitive data. In this way, we aim at making users aware of the privacy risks inherent to disclosing their data (because data are characterized and exchanged according to their sensitivity), and at balancing the reciprocal disclosure of sensitive information caused by the information exchange, thus avoiding SN free-riding. Our protocols make sensitive data release compatible with disclosure control, thereby contributing to mitigating the privacy concerns of privacy-aware users, who are especially important in SNs with sensitive scopes. Moreover, since users are rationally motivated to contribute their own private data to the network to an extent sufficient to match what they obtain from the other peers, data release becomes self-enforcing and mutually beneficial for the involved users, and sustainable in the long term.

To attain the goals above, in this work:

- We characterize the utility a user derives from participating in the SN as a function of the information she obtains about other users and the privacy risk she incurs by disclosing her own data to others. The quantification of this utility relies on an automatic assessment of the privacy risks associated to the data the SN users may disclose (*e.g.*, profile attributes, messages, etc.), which are classified according to the sensitive topic to which they refer (*e.g.*, healthcare, religion, etc.).
- We use the previous characterization to design decentralized and *co-utile* information exchange protocols, which ensure that rational users (even purely selfish ones) will follow them; that is, our protocols motivate rational users to contribute to the SN and, therefore, they thwart free-riding and ensure the sustainability of the network.
- We mitigate the reluctance of users to disclose sensitive information to others by incorporating an also decentralized and co-utile reputation system. In this way, users can build *trust* in each other, while reputation makes them accountable for their behavior. The use of reputations also makes the information exchange between peers more efficient and straightforward.
- We propose extensions to our protocols to: (i) support many-to-one information exchange (*e.g.*, within SN groups), and (ii) normalize the disclosure risk assessment (to adjust the flow of exchanged information) when applying the protocols to users with significantly different levels of social exposure (and, thus, of privacy requirements).

The rest of the paper is organized as follows. Section 2 discusses related works proposing privacy-preserving mechanisms for SNs. Section 3 presents an automatic method to measure the utility a user derives from participating in the SN, as a function of the functionality (information) she obtains from her peers and the privacy risk she incurs when disclosing sensitive data. Section 4 provides background on co-utility and proposes two co-utile information exchange protocols for SNs: a basic one-to-one iterative and incremental information exchange mechanism, and another mechanism that relies on the reputation of users. Section 5 reports the results of several experiments carried out on synthetic users and highly sensitive (health) data. Section 6 describes protocol extensions for many-to-one information exchange and for exchange between users with asymmetric social exposure. The final section gathers conclusions and identifies some lines of future research.

2. Related work

To control the disclosure of sensitive data of SN users, social network operators (such as Twitter or Facebook) have implemented basic privacy settings that enable users to specify who may access certain data, such as their profile attributes or messages. More sophisticated approaches employ privacy policies, such as contracts, which specify who can access a certain resource [7,8,15]. However, the use of manually defined privacy settings/policies has been criticized because: (i) they are burdensome to manage and, as a result, most users seldom change the default settings, that generally make most user information public [37]; and (ii) users find difficulties to assess the privacy risks caused by disclosure of their data, whereas such an assessment is needed to define access control rules [44].

Regarding this latter issue, many authors have proposed mechanisms to assess the privacy risks inherent to users' data in SNs. In [25], a privacy risk score was presented to quantify the privacy risks caused by disclosing profile attributes. Attributes (*e.g.*, country, political views, religion) are associated a sensitivity value (*i.e.*, how embarrassing it is for a user to reveal an attribute to a certain other user). The privacy score is then calculated as the sum of attributes (weighted by their respective