Information Sciences 328 (2016) 340–358

Contents lists available at ScienceDirect

Information Sciences

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

Analysis-preserving protection of user privacy against information leakage of social-network Likes[☆]

Francesco Buccafurri[a,*], Lidia Fotia[a], Gianluca Lax[a], Vishal Saraswat[b]

[a] DIIES, Università Mediterranea di Reggio Calabria, Via Graziella, Località Feo di Vito, 89122 Reggio Calabria, Italy
[b] C.R.Rao Advanced Institute of Mathematics, Statistics and Computer Science, Hyderabad, India

ARTICLE INFO

Article history:
Received 18 July 2014
Revised 10 July 2015
Accepted 20 August 2015
Available online 6 September 2015

Keywords:
Social networks
Privacy
Privacy-preserving data analysis
Partially blind signature

ABSTRACT

Recent scientific results have shown that social network *Likes*, such as the “Like Button” records of Facebook, can be used to automatically and accurately predict even highly sensitive personal attributes. Although this could be the goal of a number of non-malicious activities, to improve products, services, and targeting, it represents a dangerous invasion of privacy with possible intolerable consequences. However, completely defusing the information power of Likes appears improper. In this paper, we propose a protocol able to keep Likes unlinkable to the identity of their authors, in such a way that the user may choose every time she expresses a Like, those non-identifying (even sensitive) attributes she wants to reveal. This way, analysis anonymously relating Likes to various characteristics of people is preserved, with no risk for users' privacy. The protocol is shown to be secure and also ready to the possible future evolution of social networks towards P2P fully distributed models.

1. Introduction

Social network *Likes*, among which the most famous is the Facebook one, are a mechanism massively used by social network users to express their positive/negative association with online contents, such as photos, posts, users' status, groups, music, etc. As a matter of fact, through the above resource evaluation process, users reveal a lot of precious information, mostly unknowingly. Indeed, it is often unknown to users the possibility of predicting even hidden aspects of their own personality from digital records of human behavior. A recent study described in [44] involved 58,000 volunteers to demonstrate that Facebook Likes can be used to automatically and accurately predict highly sensitive personal attributes, including sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender. Thus, social network Likes present serious risks related to users' privacy, whose protection is more and more a salient issue, after the first Social Web era, where users seemed little careful about privacy problems. One of the reasons of this, besides personal ones, is that social networks themselves are typically designed in such a way that a user is stimulated to release private information, due to the value that such information has in term of business. As stated in [44], a distinction has to be done between the data that is actually recorded and the knowledge that can be predicted from such data, by using statistical or data mining techniques. But, whenever people have chosen not to reveal certain pieces of information about their lives, predicting them (for example, to

[☆] A shorter abridged version of this paper appears in the Proceedings of the Eleventh Annual Conference on Privacy, Security and Trust (PST 2013) [14].

[*] Corresponding author. Tel.: +39 0965 1693302; fax: +39 09651693247.

E-mail addresses: bucca@unirc.it (F. Buccafurri), lidia.fotia@unirc.it (L. Fotia), lax@unirc.it (G. Lax), vishal.saraswat@gmail.com (V. Saraswat).

http://dx.doi.org/10.1016/j.ins.2015.08.046

propose products or services) represents a dangerous invasion of privacy. For example, the positive association with a political announcement may be welcome in many cases, but it could also lead to a potentially problematic outcome in some other contexts (e.g., when it reveals the users' political leaning). Besides potential risks, we may also cite real-life events showing the dramatic consequences of a seeming innocuous click on a Like button, as the news appeared in the Washington Post that an employee logged on to Facebook and liked the page that was for a candidate challenging his boss, causing his boss to fire him from his job [40].

As it generally happens in data mining, a lot of profitable knowledge can be discovered by analyzing digital records of human behavior in social networks without breaking users' privacy. For this reason, data should be made available in such a way that only privacy-preserving analysis is possible [10,13,14,52,81]. However, the assumption that any third party which is interested to analyze data can be considered trustworthy is in fact unrealistic, due to the strategic advantage that the utilization of all data, including identifying and sensitive ones, may give to these parties. In the particular case of social network Likes, the strongest measure that can be adopted is to make Likes completely unlinkable to any attribute of people who express the association. This is what is proposed in [12], where Likes statements are treated as "light-weight e-voting procedures" in such a way that no information about the voter (that is, the author of the Like click) is related to the vote (that is, the Like). The above proposal obviously does not permit any kind of analysis about the population of users who express preferences, thus not only defusing privacy threats but also strategic analysis.

In this paper, we go one step beyond. Our proposal is still to keep Likes unlinkable to the social network profiles of their authors (and, in general to their identity), but to allow users to associate some certified attribute values with their Likes, by choosing every time they state a Like, those (even sensitive) attributes they want to reveal. From this point of view, our paper regards the topic of privacy in a weaker sense with respect to the common meaning given by the specific scientific community to this term. Indeed, we protect privacy of users by means of unlinkability to identifying attributes, not by uncertainty-based anonymization (as *k*-anonymity [69], *l*-diversity [54], or *t*-closeness [47]). Thus, even though from a merely technical perspective our solution is closer to security than privacy (in a strict sense), we refer to privacy too (in a loose sense) as, eventually, personal data of users are protected.

However, anonymous analysis relating a Like to various characteristics of the people who expressed such a preference (e.g., age, job, region, country, hobbies, etc.) is preserved with no risk for users' privacy, because there is no way to relate such information to a particular user. Observe that the above requirements evoke what is provided by selective disclosure and bit commitment approaches [8,70], but a direct application of such approaches to our case is not resolutive since the secret used by a user to enable the disclosure of the chosen attribute would allow third parties to trace the user, thus breaking anonymity. The problem is thus not trivial.

Our solution relies on a cryptographic protocol whose security is mainly based on the infeasibility of discrete logarithms and the robustness of partially blinded signatures. Moreover, we generalize the Facebook concept of Like by assuming that it is not only a positive association with an online content but also a score assigned by the user. Observe that, besides the specific not trivial requirement of linkability of Likes to only user-chosen attributes, our solution preserves the basic properties of an e-voting system as done in [12]. Indeed, whenever we implement secretness (that is, anonymity of users who express preferences) we have at the same time to avoid that users may misbehave by duplicating improperly their preference. Moreover, all the remaining basic properties of e-voting systems [19,64], namely individual verifiability, uncloneability, robustness and scalability should be guaranteed.

Our solution relies on a DHT-based P2P social network (assumed given), because we do not assume trustworthiness of the social network issuer. Consider that a recent yet consolidated scientific literature exists envisioning the new paradigm of social network shifting from client-server to P2P infrastructures, coupled with encryption so that users keep control of their information [17,18,85]. Anyway, the adoption of our model of Likes does not require a (probably unrealistic) revolution of the current social networks, as it could be implemented by distributing just the functions related to the Like expression and not the contents, possibly relying on (self-managed) cloud computing solutions.

The paper is organized as follows. In the next section, we discuss more in depth the motivations supporting our research. In Section 3, we contextualize our work in the literature giving also some important supports to our proposal. Next, in Section 4, we briefly recall some notions useful to the reader to understand the technical aspects of the paper. In Section 5, we introduce the notations used throughout the paper. The proposed protocol is described in Section 6. In Section 7, we illustrate a possible implementation of our protocol. In Section 8, the analysis of the security of this protocol is presented, by showing that all the desired features are guaranteed also against possible attacks. In Section 9, a performance analysis of the solution is provided. Finally, in Section 10, we draw our conclusions.

2. Motivations

In this section, we provide more detailed motivations that, as a side-effect, should also offer a possible business model underlying our proposal. First, we recall that our proposal comes from the need of finding a solution of the trade-off between the protection of user privacy against involuntary leakage of private information and the opportunity of exploiting digital records produced by users to make strategic analysis. We observe that both the above needs are easily recognizable as realistic, especially if we try to assume a perspective view. Indeed, what today might appear little appealing from a business point of view, tomorrow could become attractive. In our specific case, the core question is the weight that privacy will have in future business models. Likely, in a world where the digital pervasiveness will be dramatically increased together with awareness about threats