Chapter 6
An Overview on Protecting User Private-Attribute Information on Social Networks

Walaa Alnasser
Arizona State University, USA

Ghazaleh Beigi
Arizona State University, USA

Huan Liu
Arizona State University, USA

ABSTRACT

Online social networks enable users to participate in different activities, such as connecting with each other and sharing different contents online. These activities lead to the generation of vast amounts of user data online. Publishing user-generated data causes the problem of user privacy as this data includes information about users' private and sensitive attributes. This privacy issue mandates social media data publishers to protect users' privacy by anonymizing user-generated social media data. Existing private-attribute inference attacks can be classified into two classes: friend-based private-attribute attacks and behavior-based private-attribute attacks. Consequently, various privacy protection models are proposed to protect users against private-attribute inference attacks such as k-anonymity and differential privacy. This chapter will overview and compare recent state-of-the-art researches in terms of private-attribute inference attacks and corresponding anonymization techniques. In addition, open problems and future research directions will be discussed.

DOI: 10.4018/978-1-7998-5728-0.ch006

INTRODUCTION

With the increasing of information on social networks platforms, a massive amount of user-generated data online is created. This user-generated data is rich in content and includes information about users' preferences and characteristics such as geographic location, gender, occupation, and age. Therefore, user-generated data has been used by researchers and service providers to better understand users' behaviors and offer them personalized services. However, publishing user-generated data may cause the problem of user privacy as this data includes information about users' private and sensitive attributes. Private-attribute information is those that users do not want to explicitly disclose such as marital status, location, political view, occupation, age and gender. Private-attribute can be easily inferred by malicious adversaries from users' activities on online social networks. This privacy issue mandates social media data publishers to protect users' privacy by anonymizing user-generated social media data. Data anonymization is a challenging task and the ultimate goal of anonymization techniques is to prevent adversaries from inferring private-attribute by perturbing given user-generated data. Perturbing user-generated data can affect the utility of data. This leads to a dilemma between privacy and utility and makes the problem of protecting user privacy even more challenging.

There is vast literature on protecting the privacy of users in social media from two different perspectives: 1) identification of vulnerabilities and 2) mitigation of risks. The first group investigates the potential privacy breaches from social media user-generated data by introducing different variations of private-attribute inference attacks. The goal of these attacks is to identify possible vulnerabilities of user-generated data against leakage of private-attribute information. The second group seeks to mitigate existing privacy risks regarding the leakage of private-attribute by properly anonymizing user-generated data while preserving the utility of data.

Existing private-attribute inference attacks can be classified into two classes: Friend-based private-attribute attacks and behavior-based private-attribute attacks. Friend-based private-attribute inference attacks are based on the homophily theory, which implies that friends have similar attributes more than two random users. Behavior-based private-attribute inference attacks rely on inference using the similar users' behavior. They assume that similarity between users is based on their behaviors, which further indicates they share the same attributes. Besides these two classes, other approaches use both friend and behavior information to infer users' private-attribute.

Consequently, various privacy protection models are proposed to protect users against private-attribute inference attacks. These works utilize traditional privacy preserving techniques such as k-anonymity and Differential Privacy. K-anonymity (Sweeney, 2002) is one of the traditional privacy preserving techniques which seeks to anonymize the instances in the dataset by suppression and generalization. Differential Privacy (Dwork, 2008) (Dwork et al., 2006) is another traditional technique that is applied during statistical query over a dataset and seeks to improve the privacy while preserves the accuracy of results.

The purpose of this chapter is to review the existing private-attribute attacks, pointing out to the reader the different anonymization techniques to protect users' privacy as well as extend to exploring open problems and future research directions for users' privacy issues in social media. Figure 1 illustrates the objective of the chapter.