**A Survey on Privacy in Social Media - Identification, Mitigation, and Applications**

Third parties can infer the personal information like age, political affiliation and gender of the users from the publicly available user’s data. [1] [2] [3]

1 R. Dey, C. Tang, K. Ross and N. Saxena, "Estimating age privacy leakage in online social networks," 2012 Proceedings IEEE INFOCOM, Orlando, FL, USA, 2012, pp. 2836-2840, doi: 10.1109/INFCOM.2012.6195711.

2 @inproceedings{10.1145/1526709.1526781,

author = {Zheleva, Elena and Getoor, Lise},

title = {To Join or Not to Join: The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles},

year = {2009},

isbn = {9781605584874},

publisher = {Association for Computing Machinery},

address = {New York, NY, USA},

url = {https://doi.org/10.1145/1526709.1526781},

doi = {10.1145/1526709.1526781},

abstract = {In order to address privacy concerns, many social media websites allow users to hide their personal profiles from the public. In this work, we show how an adversary can exploit an online social network with a mixture of public and private user profiles to predict the private attributes of users. We map this problem to a relational classification problem and we propose practical models that use friendship and group membership information (which is often not hidden) to infer sensitive attributes. The key novel idea is that in addition to friendship links, groups can be carriers of significant information. We show that on several well-known social media sites, we can easily and accurately recover the information of private-profile users. To the best of our knowledge, this is the first work that uses link-based and group-based classification to study privacy implications in social networks with mixed public and private user profiles.},

booktitle = {Proceedings of the 18th International Conference on World Wide Web},

pages = {531–540},

numpages = {10},

keywords = {social networks, attribute inference, privacy, groups},

location = {Madrid, Spain},

series = {WWW '09}

}

3 @inproceedings{10.1145/2365952.2365989,

author = {Weinsberg, Udi and Bhagat, Smriti and Ioannidis, Stratis and Taft, Nina},

title = {BlurMe: Inferring and Obfuscating User Gender Based on Ratings},

year = {2012},

isbn = {9781450312707},

publisher = {Association for Computing Machinery},

address = {New York, NY, USA},

url = {https://doi.org/10.1145/2365952.2365989},

doi = {10.1145/2365952.2365989},

abstract = {User demographics, such as age, gender and ethnicity, are routinely used for targeting content and advertising products to users. Similarly, recommender systems utilize user demographics for personalizing recommendations and overcoming the cold-start problem. Often, privacy-concerned users do not provide these details in their online profiles. In this work, we show that a recommender system can infer the gender of a user with high accuracy, based solely on the ratings provided by users (without additional metadata), and a relatively small number of users who share their demographics. Focusing on gender, we design techniques for effectively adding ratings to a user's profile for obfuscating the user's gender, while having an insignificant effect on the recommendations provided to that user.},

booktitle = {Proceedings of the Sixth ACM Conference on Recommender Systems},

pages = {195–202},

numpages = {8},

keywords = {recommender systems, obfuscation, inference, privacy},

location = {Dublin, Ireland},

series = {RecSys '12}

}

Gender inference for Facebook picture owners

B Alipour, A Imine, M Rusinowitch

@inproceedings{alipour2019gender,

title={Gender inference for Facebook picture owners},

author={Alipour, Bizhan and Imine, Abdessamad and Rusinowitch, Micha{\"e}l},

booktitle={Trust, Privacy and Security in Digital Business: 16th International Conference, TrustBus 2019, Linz, Austria, August 26--29, 2019, Proceedings 16},

pages={145--160},

year={2019},

organization={Springer}

}

Online attacks on picture owner privacy

BA Pijani, A Imine, M Rusinowitch

@inproceedings{pijani2020online,

title={Online attacks on picture owner privacy},

author={Pijani, Bizhan Alipour and Imine, Abdessamad and Rusinowitch, Micha{\"e}l},

booktitle={Database and Expert Systems Applications: 31st International Conference, DEXA 2020, Bratislava, Slovakia, September 14--17, 2020, Proceedings, Part II 31},

pages={33--47},

year={2020},

organization={Springer}

}