Chapter 7

Retrieval of Personal Public Data on Social Networks: The Risks for Privacy

Francesca Carmagnola
University of Turin, Italy

Francesco Osborne
University of Turin, Italy

Ilaria Torre
University of Genoa, Italy

ABSTRACT

In this chapter, the authors analyze the risks for privacy coming from the distribution of user data over several social networks. Specifically, they focus on risks concerning the possibility to aggregate user data discovered on different sources into a single more complete profile, which makes possible to infer other data, likely set as private by the user. In order to show how it is possible to human users as well as to software agents crawling social networks, identifying users, linking their profiles and aggregating their data, the authors describe the prototype of a search engine they developed. The authors also present a simulation analysis to show the retrievability of user data by using a combination of people search engines and they provide statistics on the user perception on this issue.

INTRODUCTION

Online Social Networks (OSNs) allow people to publish and share information about themselves and to connect to the other members of the network. In recent years the participation in OSNs has rapidly increased. Among the top 100 most popular websites in 2102 in America, 84 are OSNs¹.

Despite the great variety of existing social networks, people using these systems share the common expectation of providing a virtual representation of themselves aimed at contacting or
being contacted by other people belonging to the network (e.g., Facebook, Classmates, Twitter), meeting new friends (e.g., Friendster, Orkut), finding new jobs or carrier opportunities (e.g., LinkedIn), sharing interests (e.g., MySpace), receiving or providing recommendations (e.g., Tribe), and so on. OSNs offer people the opportunity to establish new relationships and to interact with other people, even if far. They offer tools to foster online collaboration and facilitate the rise of new initiatives and business relationships.

Despite these interesting opportunities, there are several critical aspects. Because of the false “sense of intimacy” in social networks, people tend to be less selective in choosing the individuals to interact with and to disclose personal information more easily than in traditional relationships. Thus, a huge and heterogeneous amount of user data is scattered over social networks, including contact information, identifiable data (often published together with photographs of the subject, of her/his relatives and friends), interests, as well as political and sexual orientation, information such as current and previous schools and career, drinking and drug habits, incomes, etc. This behavior is very common among the so-called “digital natives.” Young people seem to be more relaxed in publishing intimate details of their life on the Web than “digital immigrants” (Prensky, 2004). The result is a huge amount of personal data published in OSNs with the user consent, given by accepting the policies of the social network upon registration.

However, the uncontrolled dissemination of user data can cause damages to users. In this context, the security and privacy of sensitive user information becomes a relevant issue to deal with (Ahn et al., 2011). Most of the risks are due to the lack of transparency and to the ambiguity of the data processing policy and services terms of use. Even though the Privacy Guarantees of 70 Counties (within the International Data Protection and Privacy Commissioners conference around the theme “Protecting privacy in a borderless world”) have forced OSNs to improve their privacy policies, the risk of losing the control of user data and the risk that data are shared with unauthorized third parties is still high.

Third party systems can obtain authorization from users to access their profiles for some services, gather personal private information and then use such data for different goals, that unlikely match those desired by the users, such as for marketing analyses and for advertising.

Anyone on OSNs can collect personal data and use them for purposes such as direct personal attacks, discriminations or to take on the identity of another individual (identity theft).

Recently, the profiles in OSNs are also used for social media job hunt that is for recruiting and evaluating a candidate for a job position. A research conducted between December 2011 and January 2012 showed that two out of three companies use social network profiles to evaluate and select human resources. This makes even more important to pay attention to the personal information scattered over social networks.

The focus of this contribution is specifically on the risks associated to the possibility of collecting and aggregating user data on OSNs. A paradox is that while on OSNs, and in general on social systems, users have the impression to be virtual, thanks to the multiple identities that they can easily change whenever they want, actually, following the pieces of personal information scattered across different social systems, it is possible to reconstruct their real identity. The collection and aggregation of scattered user data produces a new profile, which is more complete than the starting ones, and this richer profile may allow the inference of personal data, set as private by the user.

Moreover, it is worth noting that the insertion of data, comments and photos over time makes social systems historical repositories of the users’ activities and personal data, which often do not disappear even when the subject wishes it. The removal of the user account is rarely accompanied by a complete removal of all user-generated con-
Related Content

Regional Policy Hints from Heterogeneous Agents Simulation
www.igi-global.com/chapter/regional-policy-hints-heterogeneous-agents/29265?camid=4v1a

Civic and Political E-Participation of Young Immigrants: 'Digital Hope' for Inclusion?
www.igi-global.com/article/civic-political-participation-young-immigrants/76894?camid=4v1a

Living, Working, Teaching and Learning by Social Software
www.igi-global.com/chapter/living-working-teaching-learning-social/39730?camid=4v1a

Business Models for On-line Social Networks: Challenges and Opportunities
Omer F. Rana and Simon Caton (2010). International Journal of Virtual Communities and Social Networking (pp. 31-41).
www.igi-global.com/article/business-models-line-social-networks/49702?camid=4v1a