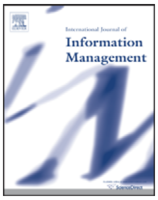
International Journal of Information Management 29 (2009) 249–254

Contents lists available at ScienceDirect

International Journal of Information Management

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



Privacy threat model for data portability in social network applications

Stefan Weiss

Goethe-University Frankfurt, School of Business and Economics, Institute of Business Informatics, Chair of Mobile Business and Multilateral Security, Grüneburgplatz 1, 60629 Frankfurt am Main, Germany

ARTICLE INFO

Keywords:
Privacy
Social network applications
Data portability
Social network portability

ABSTRACT

The advent of the participatory Web and social network applications has changed our communication behaviour and the way we express ourselves on the Web. Social network application providers benefit from the increasing amount of personally identifiable information willingly displayed on their sites but, at the same time, risks of data misuse threaten the information privacy of individual users as well as the providers' business model. From recent research, this paper reports the major requirements for developing privacy-preserving social network applications and proposes a privacy threat model that can be used to enhance the information privacy in data or social network portability initiatives by determining the issues at stake related to the processing of personally identifiable information.

1. Introduction

Privacy has been discussed in various forms and settings for more than 100 years by lawyers, philosophers, sociologists, psychologists, economists, technicians, politicians and other stakeholders. The Warren and Brandeis Harvard Law Review opinion piece in 1890, defining the right to privacy as "the right to be let alone" has set the direction for most privacy laws existing today. Alan Westin's definition for privacy in 1967 "being the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" added individual self-determination to the equation and constitutes the basis for privacy legislation such as the EU Directive[1]. Forty years later, with the advent of the participatory web and social network applications, individual self-determination once again seems to be the appropriate choice for dealing with privacy-enhanced web applications.

The extensive display of personally identifiable information (PII[2]) by users of social network applications (SNAs) on the Internet has raised concerns for privacy advocates. Additionally, while an increasing amount of privacy abuses via social network applications such as unwanted exposure, distortion, badmouthing, identity theft, cyber-bullying or reputational damage become known, the demand for serious controls to protect the individual user from any damage increasingly comes from users themselves. At the same time, SNAs have been built on top of a technology that has not been set up with lots of inherent controls. The Internet's original purpose was the openness of communication among a group of trusted people where privacy concerns did not exist.

This paper is based on research results from expert panel surveys that had been conducted in 2008 among privacy and social network application experts. The study applies a Delphi survey technique based on structural surveys and makes use of the subjective-intuitive character of the participants' answers. It is directed towards a carefully selected group of 20 technology experts who understand in depth the requirements and technical solutions for each of their specific areas of expertise, that is privacy law, security and privacy-enhancing technology, and the development of social network applications. The surveys included explorative, predictive, and normative elements and additional survey rounds with the same expert panel provided the option to give feedback from results of the prior survey rounds and, thus, enabled the validation of answers and selected solutions.

Additional sections point out the technical complexity of SNAs and the concept of data and social network portability is introduced and put in context to associated privacy risks. Finally, a privacy threat model for data portability in social network applications is proposed. It can be used to enhance the information privacy in data or social network portability initiatives by determining the issues at stake related to the processing of personally identifiable information.

E-mail address: stefan.weiss@m-chair.net.

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, in *Official Journal of the European Communities*, November 23, 1995, No L. 281 p. 31.

[2] Personally identifiable information (PII) is defined in this paper as being any information (a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains, (b) from which identification or contact information of an individual person can be derived, or (c) that allows linking particular personal characteristics or preferences to an identifiable person.

0268-4012/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ijinfomgt.2009.03.007

2. Requirements for privacy-preserving social network applications

The rising use of SNAs on the Internet is a phenomenon that left lots of privacy advocates puzzled. Personally identifiable data that was sought to be at the core of any privacy-enhancing technology and needed to be encrypted, hidden or anonymized are nowadays provided willingly by users of social network sites (Kolbitsch & Maurer, 2006). Recent privacy studies for online communities, however, reveal the fact that most users are unaware of specific risks of privacy-invasive activities and have no idea to what degree their online profiles and the PII connected to it is visible and exposed to others (Acquisti & Gross, 2006). A fact that also explains results from user surveys where users always say they are clearly concerned about their own privacy but then make decisions to reveal PII data about themselves that are contradictory to their concerns for privacy (Flinn & Lumsden, 2005). Acquisti and Grossklags (2004) have elaborated on this dichotomy between privacy attitude and behaviour and concluded that individuals are neither able to calculate the probabilities and amounts of risks nor are they able to perceive the long-term risks and losses while acting in privacy-sensitive situations.

The usage of SNAs presents such a privacy-sensitive situation in which a great amount of PII is revealed to others. For the expert research, it was presumed that social network users are not aware of the risks to their information privacy and, therefore, survey users' preferences, attitudes and behaviour were not examined in more detail. Instead, a group of individuals who were considered experts in their respective fields of work were assembled and surveyed about their opinions and suggestions for effective solutions.

The research, based on a Delphi survey technique, had the objective to aggregate expert opinions and arguments on the most pressing challenges when trying to enhance the information privacy for users of social network applications. Privacy experts with a legal, technical and business background from countries in Europe, North America and Asia were asked to be on the expert panel. All of them had a particular experience in dealing with SNAs either from their academic, private company or public sector positions.

The research results are twofold. In a first expert panel survey with 41 structured questions, the major privacy concerns, the effectiveness of possible solutions, and the requirements for developing privacy-preserving SNAs among other topics were explored. A second expert panel survey tried to validate the proposed privacy solutions. From the analysis of the first round of expert panel surveys, the following factors depicted in Table 1 seem to influence the development and operation of privacy-preserving SNAs.

2.1. Major concerns

The experts were asked to pick the major privacy concerns they see in using SNAs. The top ranked answers for the major concerns are related to the lack of self-control and transparency to the user. These concerns support earlier findings where privacy is affected by the users' inability to control impressions and manage social contexts, for example with the early introductions of such features like "News Feed" and "Beacon" in the Facebook application (Boyd & Ellison, 2007). Furthermore, the surveyed experts see a major concern for the information privacy of users in the combination of an immature technology on the one side and providers on the other who need to proof their business model by further expanding ways to exploit the value of their users' PII.

2.2. Possible solutions

When asked about effective solutions it is interesting to note that proposed privacy-preserving solutions for using the Internet at large was quite different than the proposed solutions for SNAs. In the first case, traditional privacy-enhancing technologies (PETs) such as providing options to use pseudonyms, anonymization techniques, and data access rights management were priority. For social network applications possible solutions focused on transparency, automated compliance functions, and proactive communication techniques that can build awareness about potential risks. Those choices suggest that the expert group sees a distinct difference between Internet communication where traditional PETs can assure some level of privacy and social networks where the proliferation of PII is at the core of the underlying business model.

2.3. Requirements

The survey answers that were analyzed for this journal contribution are related to an importance ranking on a 5-point Likert scale. The experts were asked to rank the importance of a list of requirements for fostering the privacy-preserving use of social network applications. The result revealed that nearly 87% of the respondents see privacy-by-design practices for web designers and developers as the most important requirement for privacy solutions to work. This result is also supported by requirements set for ubiquitous computing systems where a comprehensive set of guidelines for designing privacy-aware ubiquitous systems were suggested (Langheinrich, 2001). Further requirements for fostering a privacy-preserving SNA were transparent and open privacy handling practices and options for the user to easily report privacy invasions.

Other frameworks for analyzing requirements for privacy-preserving social networks have been suggested (Preibusch et al., 2007). However, they concentrate on privacy in the sense of data protection, i.e. as a restriction on data access and data processing and not so much on the transparency and control mechanisms that need to be developed.

The expert panel survey findings reveal an interesting point: the survey participants see the open nature of SNAs and their underlying database infrastructure as a given and suggest new forms of privacy-preserving mechanisms to solve the information privacy concerns inherent in such an environment. Privacy-by-design at the application development stage becomes more important. But the general call for more transparency, more structure and more control for the individual user is probably the greatest challenge for developers and providers alike. Especially because more than half of the surveyed experts attested an extremely low confidence

Table 1
Factors influencing the development of privacy-preserving social network applications.

	Major concerns	Possible solutions	Requirements
Rank 1	Having no control over usage and proliferation of PII	Complete transparency over the usage of one's own PII	Privacy-by-design practices for web designers and developers
Rank 2	No transparency on what happens with PII	Privacy policies with an automated compliance assurance function	Transparent and open privacy handling practices
Rank 3	Unauthorized third party use of PII	Proactive and automated communication techniques on risks	Options for the user to easily report privacy invasions