Journal of Information Security and Applications 000 (2017) 1–15

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

A greater understanding of social networks privacy requirements: The user perspective

Mohammad Badiul Islam[a,b,*], Jason Watson[b], Renato Iannella[b], Shlomo Geva[b]

[a] Data61, CSIRO, Brisbane, Australia
[b] Queensland University of Technology (QUT), Brisbane, Australia

ARTICLE INFO

Keywords:
Users privacy
Social networks functionality
Information disclosure
Thematic analysis
Privacy requirements
Privacy concerns

ABSTRACT

Social Networks (SN) require an accurate understanding of the complex privacy requirements of users to demonstrate respect for user privacy requirements whilst also encouraging sharing. This research extends current understanding of SN user privacy requirements using the PREview approach, drawing on a thematic analysis of related scholarly articles and validating and extending themes by survey. The findings instantiate five primary privacy requirements including: Information Control, Information Collection and Storage, Information Access, Secondary Use, and Social Network Practice, and a further twenty five secondary requirements. This research has the potential to assist with the development of enhanced SN privacy controls.

1. Introduction

Social Networks (SNs) are designed as public spaces for the private individual [1]; however, since individuals use these public spaces to disseminate their personal information, the networks become the source of complex privacy concerns. Privacy has become a significant contemporary issue [2] in SNs due to the massive sharing and exchange of personal information such as pictures and online activities. For example, inappropriate usage, such as connecting contacts without confirming identity, may lead to serious scenarios.[1,2] SN users have become more aware of privacy concerns and consequently, that this could affect their future SN engagement.[3]

The motivation for this paper arose out of SN privacy concerns we experienced and documented by analysts, researchers, and SN users. All of these are (somehow) about privacy and the design of the system [3]. For example, Solove [4] provides a catalogue of activities that may lead to privacy breaches and concerns. Prior studies inadequately established the benefits of improving the system design from a focus on privacy notions (legal [4–7] and surveillance studies [8–12]), various privacy solutions (Islam et al. [13], Islam [14] list various existing privacy solutions) in particular during requirements engineering in a SN context [3].

Embedded Privacy by Design (PbD) [15] principles at the design level specifically during requirements engineering of SNs architectures could be the solution for ensuring privacy from the beginning of a system's development [2,13]. In doing so, it determines the issues that need to be addressed in this area to improve the design of the system to deal with the privacy concerns while design and developing system specially during requirements engineering [3].

Zave and Jackson [16] identified that the outstanding problem area of enterprise as "generating strategies for converting vague goals (e.g. "user friendliness", "security", "reliability") into specific properties or behaviour", in particular, where the vague goals are critical to the success of the enterprise [17]. So, Zave and Jackson [16] defined requirements as the system-to-be in which specified machine (system) (i.e. SNs platform) interacts with the given surroundings (environment) (i.e. social context) such that a set of desired conditions hold. Privacy requirements can also be captured as a set of concepts relate to stakeholder privacy concerns with respect to a system-to-be, to privacy goals (i.e. anonymity in confidentiality) and privacy constraints (i.e. confidentiality constrains due to collection of surveillance information for possible (unwanted) inferences) [3] instead of vague goals. However, SN is hindered by a lack of empirically validated yet actionable sin-

* Corresponding author.
E-mail addresses: badiul.islam@data61.csiro.au (M.B. Islam), ja.watson@qut.edu.au (J. Watson), r@iannel.la (R. Iannella), s.geva@qut.edu.au (S. Geva).

[1] Facebook "Friends" Murder 25-Year-Old Girl: http://news.peacefmonline.com/news/201208/130827.php

[2] Coeburn police officer accused of soliciting sex from 15-year-old girl: http://bit.ly/accusedofsolicitingsex

[3] http://www.quitfacebookday.com

http://dx.doi.org/10.1016/j.jisa.2017.01.004
2214-2126/

gle framework through different privacy notions that evolved the stakeholder concerns and requirements can be translated into the system-to-be during requirements engineering [3].

A variety of methods may be suitable in exploring SN user privacy requirements; each has its advantages and drawbacks. For example, findings from [18] suggest that case study method is the most widely used to investigate contemporary phenomena within certain real-life contexts where the investigator has little control over the events. A case study typically uncovers what is actually there, and the existing or missing features which users may be aware of. SN user privacy requirements may be uncovered in a case study; however, many privacy requirements are not addressed at all by typical social networking sites and cannot be uncovered from a study of existing systems.

After experiencing these difficulties, we elected to design a new and more fine-grained research model. Following Sommerville and Sawyer [19], we use SN user privacy concerns to synthesise SN user privacy requirements based on PREview viewpoints model which uses stakeholder concerns to reflect critical non-functional characteristics of a system [19] to discover system requirements. This research is also inspired by the Gürses [3]'s multilateral privacy requirements analysis and develop a research model that combines mixed methods research employing the strengths of quantitative and qualitative research to explore the SN privacy requirements.

This paper is structured as follows. In the next section the related works are discussed. We then describe the research model used and the process for constructing SN user privacy requirements.The following section presents the validation of the SN user privacy concerns with analysis and the results and SN user privacy requirements. The final section concludes with the paper summary.

2. Related works

Privacy requirements can be explored from a variety of perspectives such as confidentiality requirements engineering [20], security engineering method by exploring security properties e.g., confidentiality, anonymity, unobservability [21–23] based on the concept keeping information confidential as not being collected, minimised collection, anonymised, unlinkable or unobservable. However, privacy is not simply the hiding of information; it is also the legitimate control over one's own personal information. Without an individual's explicit consent, nobody has the right to access another's personal information unless there are laws permitting access to that information; for example, tax authorities may have access to income information from employers.

Privacy requirements can also be derived from data protection legislation, communicated through (legal) privacy policies [24,25] and make systems data protection legislation compliant [26,27]. Prior research has shown that comparable problems arise when data protection legislation is translated into system requirements [26,28,29]. Further, these authors and Gürses [3] emphasis that privacy requirements elicited from data protection means that they focus on organisational compliance. Such an approach may disregard the subjectivity of privacy for end-users and other stakeholders as a result of their focus on organisational compliance to legal frameworks.

Recent research has also shown that comparable problems arise when data protection legislation is translated into system requirements [26,28,29]. Further, these authors' emphasis on privacy requirements elicited from data protection means that they focus on organisational compliance. Such an approach may disregard the subjectivity of privacy for end-users and other stakeholders as a result of their focus on organisational compliance to legal frameworks.

Following Gürses [3], privacy requirements may rely on counter-factual arguments about privacy or privacy breaches and concern (counter-factuality). In logic, a counter-factual conditional is a conditional (if-then) statement indicating what would be the case if its antecedent were true. For example, "human are mammal" and "mammal cannot flies". The idea is that if we know that *X* is a mammal then we may conclude that it cannot fly *unless there is other, not inferior, evidence suggesting that it may fly* (for example that mammal is a bat). Similarly, if privacy requirement "R" as constraint was not satisfied then privacy concern "C" may occur. However, such a counter-factual relationship is hindered by a lack of a deeper analysis of assumptions, facts and even other counter-factuals.

There are various dimensional or factorial models available for representing privacy concerns. For example, "Model 1" – a one-dimensional (one factor) model – is a plausible model underlying data structure [30]; this model can assess the level of concern about an issue using an option survey such as, "*How concerned are you about threats to your privacy in America today?*" [31]. "Model 2" is a two-dimensional (two-factor) model where privacy concerns can be measured as both "information collection" and "maintenance of that information" [32]. "Model 3" is three-dimensional (three-factor), where privacy concern can be reflected into "information collection", "information management" (which includes errors and unauthorised access), and "secondary use" [32].

To this end, after analysing the literature of privacy requirements and concerns in SNs, we can observe that this area is still an open domain for research and analysts, researchers and SN users are expressing their concerns about these requirements, and are engaging in attempts to mitigate these concerns. While SN service providers offer various services and functions – such as "edit", "share", "export", "delete" various types of SN data and information– it is often not clear what rights SN users really have [33] and which dimensional or factorial models are appropriate for representing SN user privacy concerns and requirements. For example, users may wish: to delete their various types of private information, or control information sharing as their privacy requirements; to control access to some types of information but disclose other types of information; or to share information with one particular stakeholder, while restricting it to others. SN users may wish to share their information with individual stakeholders or share among a particular group. However, in the current paradigm, social networking sites have become a centralised system based platform that does not allow full control over individual information or practice of that control. This research focused, therefore, on investigating systematically user privacy concerns and requirements from various SN stakeholders.

3. SN user privacy requirements construction process

We used a empirical research approach to explicate the requirements and theoretical principles for a new multilevel model for measuring and validating the SN user privacy concerns and eliciting SN privacy requirements.

3.1. Research model

Initially we identify SN user privacy concerns which affect the SN privacy goals. Then we elicit SN user privacy requirements based on PREview (*P*rocess and *r*equirements *e*ngineering *view*points) approach [17,19]. The PREview approach is a spiral process, which emerges from successive iterations of the three basic activities performed each cycle, which are "Requirements elicitation", "Requirements analysis" and "Requirements negotiation [17] in a context of a particular viewpoint. The Requirements elicitation express the organisational needs, which is a systemmatic approach to explore the system requirements. Oftenly, the system

Please cite this article as: M.B. Islam et al., A greater understanding of social networks privacy requirements: The user perspective, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.01.004