Colour as an Indicator of Vulnerability of Users Within Social Networks

Amanda Cox, Charles Sturt University, Wagga Wagga, Australia
Yeslam Al-Saggaf, Charles Sturt University, Wagga Wagga, Australia
Kate McLean, Charles Sturt University, Wagga Wagga, Australia

ABSTRACT

Social networking users are presented with a plethora of profile and privacy settings; most of which are left defaulted. As a result, there is little understanding of the fields that make up the user profile, the privacy settings available to safeguard the user, and the ramifications of not changing the same. Concerns relating to the unprecedented quantities of Personally Identifiable Information being stored need to be addressed. By employing a risk matrix to a social media profile, a user could be alerted to the potential dangers of the information being contained within the profile. By adapting this tool, the risks to the individual user of a social media profile will be minimised.

KEYWORDS

Colour, PII, Privacy, Risk Matrix, Social Networks

INTRODUCTION

On any given day we find ourselves stopped at a stop sign or a traffic light. We have been educated that a red signal means STOP or DANGER. Can this logic be applied to a social networking environment? A related question is to what extent a social media user’s Personally Identifiable Information (PII) can be protected by applying a colour code to indicate the danger of disclosing a user’s PII? The extant literature highlights the plethora of privacy issues facing social media users and it is generally acknowledged that the onus of protecting privacy is on the user.

Previously proposed solutions, such as those outlined by Ge and Zhu (2011), include the application of complex algorithms such as Trust Third Party, Data Perturbation Technique, Secure Multiparty Computation and Game Theoretic Approach to perform privacy preservation of PII. The methodology that Ge and Zhu (2011) suggest removes the user’s involvement. Thus vulnerability is potentially increased as users are not aware of the amount of (PII) held within their user profile. Many empirical studies have been conducted in the area of social networking sites (SNS). Sar and Al-Saggaf (2014) identified that the focus of these studies should include the privacy of user information and how this is shared over these sites, with or without user awareness or consent.

There are many considerations and risks associated with the social media applications for personal use. By employing a risk matrix to a social media profile, a user could be alerted to the potential dangers of the information contained within a profile.

Social media profile structures are multifarious to the average user, and much of the data captured is “hidden” within the profile. Thus, the main research question is:

To what extent can the privacy of Personally Identifiable Information within social networks be improved/protected by adapting a risk matrix as a tool to generate a value to indicate a use of colour?

This study allows user involvement, by showing the user the extent of their vulnerability. By displaying the level of vulnerability through colour-coding, the risks associated with “completing” a user profile will be mitigated.

DOI: 10.4018/IJSKD.2016010104

Copyright © 2016, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
This paper comprises the following sections:

I. a brief background of the privacy issues surrounding social networks,
II. a description of the methods to devise a risk matrix to support the study, and
III. the methodology used to gather the data to develop a prototype of the risk matrix.

BACKGROUND

Facebook

Originally intended as a personal space to share information about oneself; Oeldorf-Hirsch and Sundar (2014) believe that Facebook has become a common venue for sharing external content with one’s network. Baresh, Knight, Harp and Yaschur (2011) concur and enhance the sentiment by inferring that Facebook has become one of the leading referrers to news sites through links shared by friends when it comes to news items.

Sundar (2008) believes that Facebook encourages content distribution by making communication features such as status updates, photo and video-sharing options, and location check-ins prominent and easy to use. Van Dijck (2013, p. 12) states by “technologically encoding people’s activities; formal, manageable, and manipulable, enabling platforms to engineer the sociality in people’s everyday routines”. Anderson (1997) touts the use of any media has the ability to be added to the norms, values, ritual, custom and language to modernised a culture.

Van Dijck (2013) also postulates that the use of Facebook will lead to the creation of a transparent social world where users act as a source of information allows users to experience a sense of agency by feeling that they have some control over information on the site.

With the abundance of information available on social networks, in particular, Facebook, a user may become overwhelmed and is, therefore, unlikely to realize the amount of personal information they have divulged.

Privacy Paradox

Privacy issues become all the more important as availability of publicly shared personal information is increased. Social media and networks facilitate an unprecedented level of accessibility and transparency. Facebook users express concern about the publication of personal information in the online environment, but at the same time, as Boyd (2007) states, users actively construct their identity online through the disclosure of personal information. There are many reasons for the increased risk of personal information being used for purposes other than that originally intended on social network sites. Fuchs (2010) indicates that Facebook’s idea of privacy is based on an understanding of self-regulation and an individualistic perspective of privacy.

Dumas, Serfass, Brown and Sherman (2014, p. 376) state “users should not bear the entire burden of their privacy protection”, especially when SNS dictate the terms of the agreement. Social networking users sacrifice privacy the very moment the “I accept” button is pressed. User data is used as a commodity for sharing with third parties, mainly advertisers. The problem Fuchs (2010, p. 148) describes “is that the users are not asked if they find targeted advertising necessary and agree to it”. This technique uses the concept of ‘user consent’ in Facebook’s Privacy Policy.

A sharp juxtaposition exists between the concern people express and their readiness to disclose personal information. Barnes (2006) has identified these phenomena as “the privacy paradox”, a finding that has shown how, despite expressing a concern about Facebook privacy, people often do very little to protect themselves. Boyd (2006) cautions that social media users should think twice
Knowledge Management in Virtual Enterprises: Supporting Frameworks and Enabling Web Technologies
[www.igi-global.com/chapter/knowledge-management-virtual-enterprises/6013?camid=4v1a](www.igi-global.com/chapter/knowledge-management-virtual-enterprises/6013?camid=4v1a)

Balancing McLuhan With Williams: A Sociotechnical View of Technological Determinism
Liza Potts (2013). *Knowledge and Technological Development Effects on Organizational and Social Structures* (pp. 109-114).
[www.igi-global.com/chapter/balancing-mcluhan-williams/70565?camid=4v1a](www.igi-global.com/chapter/balancing-mcluhan-williams/70565?camid=4v1a)