Translating IUIPC into Design: The Case of Third-Party Applications on Facebook

Na Wang, Heng Xu, and Jens Grossklags
The Pennsylvania State University
University Park, PA 16802 USA
nzw109,hxu,jens@ist.psu.edu

Abstract
This research attempts to map the measurement of Internet Users' Information Privacy Concerns (IUIPC)[7] to the design of privacy notice dialogues for third-party apps on Facebook. Specifically, we propose two improved designs of privacy notice dialogues to encompass *control* and *awareness* as the essential factors to address users' privacy concerns toward third-party apps on Facebook. The approach of Privacy by ReDesign is employed to investigate whether users can more adequately represent their preferences for sharing and releasing personal information with these two improved designs.

Keywords
Internet Users' Information Privacy Concerns (IUIPC), Third-Party Applications; Facebook; Privacy Notice

ACM Classification Keywords
D.4.6 [Security and protection], H.5.2 [Information interfaces and presentation]: User Interfaces - Evaluation/methodology

Introduction
The extensive disclosure of personal information by users of social networking sites (SNS) has made privacy concerns particularly salient. The growth of apps' aggressive practices of collecting users' information from SNS (e.g., Facebook) made this situation even worse. A heightened need for empowering user control for third-party apps arises due to the inability to monitor the data use by app providers within and outside of the social networking platform and the inherent uncertainty about their privacy practices.

In this research, we aim to protect users' information privacy associated with their use of third-party apps on a specific social networking platform, namely, Facebook. We implement the theoretical framework

Figure 1. Original Design of the Privacy Notice Dialogue on Facebook

developed by Malhotra *et al*. [7] into our design paths intended to produce two improved designs of privacy notice dialogues that are specific to Facebook. Our new designs encompass *control* and *awareness* as the essential dimensions of users' privacy concerns in the context of third-party apps on Facebook. We aim to examine the extent to which users can more adequately represent their preferences for sharing and releasing personal information by using our new interface designs of privacy notice dialogues.

Conceptual Foundation

Privacy by ReDesign

According to Cavoukian and Prosch [3], "[t]he reality … is that it is not always possible to embed privacy directly from the outset." System improvements are incremental, seldom revolutionary. As a result, the integration of privacy enhancing features into existing systems often happened using an ad hoc approach. In this work, we believe that the notion of Privacy by ReDesign can be well applied to the platform of Facebook, as it constantly changes its specific features and interface details while aiming for a consistent and recognizable overall user experience. As a result of rapid network growth, a careful design of appropriate privacy features from the outset was likely not always prioritized. However, as a more mature platform, pressure from users and regulators or novel business needs (e.g., in the case of third-party apps) lead to a re-examination and successive iterative improvements of existing privacy enhancing features.

Design Principles

In this research, we ground our work in the theoretical framework of IUIPC and attempt to map these three dimensions of users' privacy concerns to the design of privacy authorization dialogues for third-party apps on Facebook. Specifically, the original design of the privacy notice dialogue employed by Facebook (see Figure 1) has addressed the *collection* dimension of IUIPC by providing a basic notification that users' personal data are being collected. However, prior research has pointed out that such an interface to notify users about the app's information practices is uninformative and ineffective. Besmer and Lipford [2] suggest that Facebook users are not truly understanding and consenting to the risks of apps that maliciously harvest their profile information. To address these limitations, we argue that an effective design of a privacy notice dialogue should further address the *control* and *awareness* dimensions of IUIPC. To accomplish our goals of Privacy by ReDesign, we first inscribe theoretical elements in the ensemble artifact (i.e., new interface of privacy notice dialogues).

EMPOWERING USER CONTROL

Constituting the "active" component of privacy concerns, control refers to the degree individuals perceive themselves to be vested with power over the procedures [7]. Evidence suggests that issues with information access and usage are more appropriately managed through "control over who has access to personal data, [and] how personal data are used" [8, p.29]. In the original design of privacy notice dialogues on Facebook, users do not have any control to limit the app's access to their information or restrict app's use of their information during the process of adding an app to users' profiles [9]. Only after they add the app, users could potentially edit selected categories of information access or use if they found the relevant options deeply buried in their global privacy settings [9].

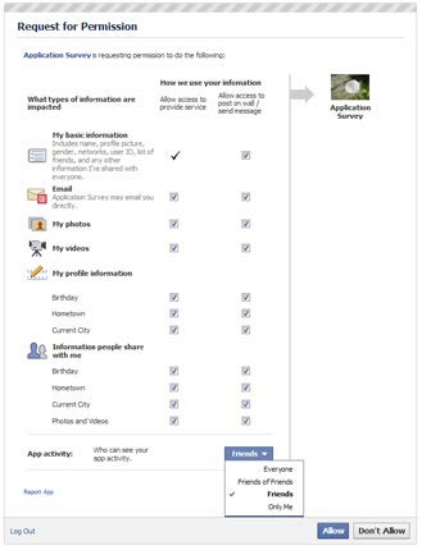

Figure 2. Proposed Design for Empowering Control.

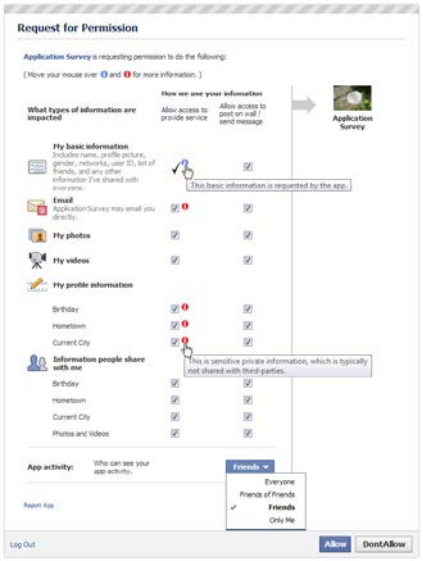

Figure 3. Proposed Design for Promoting Awareness.

To address these limitations, app providers should explicitly provide users with different options for disclosing different types of information, as well as clearly differentiate the purposes of data permissions. Below we describe our new design to empower user control (shown in Figure 2):

• *The Layout of Individualized Permissions:* All types of data (basic information and extended data permissions) required by an app are listed in the first column. The first row displays the purposes of information use (including data writing and data reading). Our design decision to employ this layout of individualized permissions is consistent with many other studies that have proposed ways to improve on text-heavy privacy policies [6]. The core solution from this stream of literature is to use tables or grids to distill various choices into more readable and user-friendly formats.

• *The Tick Mark and Checkbox*: Un-clickable tick marks represent those types of information that will be accessed by the app. This category of data access is non-negotiable (e.g., because of functional requirements). The checked checkbox means that users will allow the app to access and use certain information. When un-checked, users will prevent the app from accessing or using the corresponding information.

PROMOTING PRIVACY AWARENESS

Constituting the "passive" component of privacy concerns, awareness is related to an individual's knowledge of the relevant privacy context such as organizational privacy practices for online commercial transactions. Awareness provides individuals with justifications for how information is exchanged and explanations for why certain information is requested [4]. If individuals are deprived of these contextual information, privacy concerns would prevail [5]. Malhotra *et al*. thus suggest that awareness can be manifested as informational justice which emphasizes on the articulation of information [7]. In the context of Facebook, users may easily give out their sensitive private information to third-parties, with which users' crucial identity information can be predicted. For example, information about an individual's date and place of birth can be exploited to predict his or her Social Security number [1]. In the original design of privacy notice dialogues on Facebook, there is no warning mechanism to alert users when their sensitive private information is being requested by the apps.

We consider promoting awareness to be supplementary to empowering control in that it helps users to make meaningful choices over the now individualized control elements. As a result, we redesign the privacy notice dialogue to combine the elements of empowered control and increased awareness (shown in Figure 3). We expect such merged design to effectively address the complexity of the privacy decision-making problem.

• *The "i" Mark and Color Scheme*: The blue "i" mark reminds users that the basic information bundle is requested by the app and users cannot opt out from this part of the information request. The red "i" mark alerts users that certain private information is particularly sensitive, and is typically not shared with others. Both blue and red "i" marks have tooltip information provided to the user when they mouse-over the sign. In this study, our design decision on the red "i" mark was based on Acquisti and Gross's finding that information about a user's place and date of birth can be exploited to predict the user's Social Security number [1].

Empirical Investigation: Ongoing Research

At this CSCW workshop, we will be able to demonstrate the prototype together with preliminary user evaluation results. In future work, we expect to extend these investigations, complete the prototype implementation, and iterate on our empirical investigations.

References

[1] Acquisti, A. and R. Gross, *Predicting Social Security numbers from public data.* Proceedings of the National Academy of Sciences, 2009. **106**(27): p. 10975.

[2] Besmer, A. and H. Lipford. *Users' (mis)conceptions of social applications*. in *Proceedings of Graphics Interface (GI'10)*. 2010. Ottawa, Canada: Canadian Information Processing Society.

[3] Cavoukian, A. and M. Prosch. *Privacy by ReDesign: Building a Better Legacy*. 2011; Available from: http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1070.

[4] Colquitt, J., A. , D.E. Conlon, M.J. Wesson, C. Porter, and K.Y. Ng, *Justice at the Millenium: A Meta-Analytic Review of 25 Years of organisational Justice Research.* Journal of Applied Psychology, 2001. **86**(3): p. 425-445.

[5] Hoffman, D.L., T.P. Novak, and M.A. Peralta, *Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web.* Information Society, 1999. **15**(2): p. 129-139.

[6] Kelley, P., J. Bresee, L. Cranor, and R. Reeder. *A Nutrition Label for Privacy*. in *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS)*. 2009. Mountain View, CA.

[7] Malhotra, N.K., S.S. Kim, and J. Agarwal, *Internet users' information privacy concerns(IUIPC): the construct, the scale, and a causal model.* Information Systems Research, 2004. **15**(4): p. 336-355.

[8] Phelps, J., G. Nowak, and E. Ferrell, *Privacy Concerns and Consumer Willingness to Provide Personal Information.* Journal of Public Policy and Marketing, 2000. **19**(1): p. 27-41.

[9] Wang, N., H. Xu, and J. Grossklags. *Third-Party Apps on Facebook: Privacy and the Illusion of Control*. in *Proceedings of the ACM Symposium on Computer-Human Interaction for Management of Information Technology (CHIMIT)*. 2011. Boston, MA.