Workshop on the Future of Privacy Notice and Choice
Carnegie Mellon University, Pittsburgh, PA
June 27, 2014

# Default and Context: Investigating Facebook Users' Privacy Perceptions and Behaviors of Installing Third-Party Apps

Heng Xu, Na Wang, Pam Wisniewski, and Jens Grossklags

**ABSTRACT**
Through a controlled experiment of 298 Facebook users, we examined how varying the default settings of the privacy notice dialogue, presented during the app authorization process, and the context of a third-party application influence users' privacy perceptions and information disclosure behaviors. In our between-subject design, we provided three variations of default privacy settings (Opt-In, Minimally Necessary and Opt-Out), and two app contexts (e.g. Photo App and Birthday App). We found when participants perceived the app were asking for more than necessary information, they tended to have more negative impression over the app and deny installing it to prevent their information from being released. Our Results also indicated that participants had more concern over releasing unnecessary photo-related information than birthday-related information.

**INTRODUCTION**
Facebook, the largest SNS, currently has 1.11 billion monthly active users [4], representing approximately 92% of all SNS users [9]. According to Facebook Statistics, over 10 million applications (apps) [10] are available on this platform, and 1 in 4 Facebook users install these apps [1]. However, most users do not understand how apps work, what information they can access, or how they are developed and reviewed [5]. Further, privacy incidents have raised concerns about Facebook's data practices. For example, the Wall Street Journal reported that many Facebook apps transmit personally identifiable information of tens of millions of Facebook users to advertising and marketing companies – without their knowledge [11].

A growing body of literature has tried to address the problem of information collection by third-party apps through providing users with additional options for privacy control [12, 13, 14]. However, the results of this approach have varied. For example, one study found that allowing for granular control of privacy settings resulted in fewer participants installing an app [2]. It is possible that more choices, while increasing control, also increase users' cognitive costs and lead to choice overload. Therefore, empowering users with additional choices may not be a sufficient solution by itself. We study an alternative approach. We enhance the design of privacy notices with appropriate default settings so that only the information needed by an app is shared. This approach both facilitates users' control by providing more options and reduces cognitive load by suggesting appropriate privacy defaults

We use an experimental design to manipulate the default privacy settings for the types of information the app intends to access (Opt-In, Minimally Necessary, and Opt-Out) as well as the context (Photo App vs. Birthday App) in which Facebook users make privacy decisions. We assess how users perceive the usefulness and the potential threat of these varied default privacy conditions. Our experimental study will help us answer the following important research questions:

- How do different *default settings* of privacy notice dialogues affect users' information disclosure behaviors and privacy related perceptions?
- How does the *context* of an app affect users' information disclosure behaviors and privacy related perceptions?
- How does the *app context across different default settings* of privacy notice dialogues affect users' information disclosure behaviors and privacy related perceptions?

By better understanding SNS users' information disclosure behaviors and privacy perceptions across different contexts and attributes, SNS service providers will be able to provide users with more reliable mechanisms for making informed privacy decisions when sharing information through third-party apps. We are unaware of any researchers that have performed controlled experiments to evaluate the impact of different types of default settings and app contexts on users' decision making in the domain of SNS. Therefore, this is a unique contribution of our work.

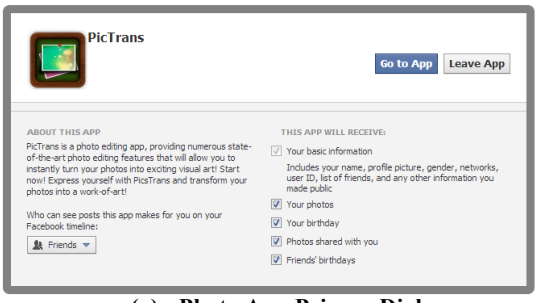
**METHODOLOGY**
We conducted an online, between-subject experiment using a combination of the Facebook Application Platform, Google Chrome browser extensions, and Amazon Mechanical Turk.

**Experimental Design**
*Privacy Setting Defaults*
We chose to examine three different levels of ***privacy default settings***: 1) Opt-In (**IN**), 2) Minimally Necessary (**MIN**), and 3) Opt-Out (**OUT**). For the opt-in condition, none of the information was selected to share by default, while all of the information was selected to share by default for the opt-out condition. For the minimally necessary condition, we drew from the theory of contextual integrity [7], which suggests that the relevance of information, in respect to the situational ***context*** and the information ***attributes*** (type of information being shared), are two key parameters in terms of how individuals develop their

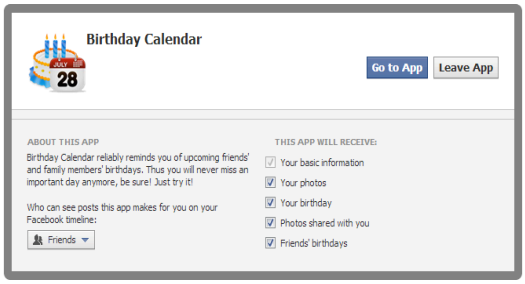
privacy expectations and norms [7]. Therefore, minimally necessary privacy defaults would only share information relevant to the app by default, and the amount of information disclosed by default across these three levels of privacy default settings would be characterized as: *IN* < *MIN* < *OUT*, respectively.

*App Context*

We varied ***app context*** by telling participants that they were installing one of two different types of apps: 1) A Photo App (**P**), or 2) A Birthday App (**B**). **Figure 1** shows an example of the prototypes of our privacy notice dialogues for both the Photo App ("PicTrans") and the Birthday App ("Birthday Calendar"). In all conditions, the privacy notice dialogue requested five types of information: 1) Basic Information, 2) Photos, 3) Birthday, 4) Friends' Photos, and 5) Friends' Birthday. Users were able to change the default privacy settings for all types of information being requested except for Basic Information, which is required for all third-part apps.




**(a) Photo App Privacy Dialogue**




**(b) Birthday App Privacy Dialogue**

**Figure 1: Chrome Extension Prototypes of the Privacy Notice Dialogues.**

Given our two levels of app context (Photo App and Birthday App) and three levels of privacy default settings (Opt-In, Minimally Necessary, and Opt-Out) as described above, we employed a 2 X 3 between subject design, holding the information attributes requested by the app constant across all six conditions but changing the privacy defaults. **Table 1** summarizes our 2 X 3 between-subject design.

### Procedure

To implement our design, we developed a Chrome browser extension to override Facebook's default privacy notice for adding new Facebook apps. We followed the experimental procedure we established in [12]: First, pre-screened MTurk participants began the study by taking a pre-survey that captured various individual characteristics, such as demographic information and general privacy concerns. Second, participants were asked to install our Chrome browser extension. Third, participants were randomly assigned to one of the four experimental conditions shown in **Table 1**. Depending on the condition assigned, participants were presented with a privacy notice, where they were able to customize privacy settings prior to making an installation decision. After customizing the default privacy settings and deciding whether or not to install the app, participants were redirected to a post-installation survey which asked about their interactions with and perceptions of the privacy notice.

**Table 1. App Context (P, B) and Default Settings (IN, MIN, OUT) 2 X 3 Experimental Design**

| | **Photo App (P)** | **Birthday App (B)** |
|---|---|---|
| **Opt-In (IN)** | THIS APP WILL RECEIVE:<br>☐ Your basic information<br>☐ Your photos<br>☐ Your birthday<br>☐ Photos shared with you<br>☐ Friends' birthdays | THIS APP WILL RECEIVE:<br>☐ Your basic information<br>☐ Your photos<br>☐ Your birthday<br>☐ Photos shared with you<br>☐ Friends' birthdays |
| **Minimally Necessary (MIN)** | THIS APP WILL RECEIVE:<br>☐ Your basic information<br>☑ Your photos<br>☐ Your birthday<br>☑ Photos shared with you<br>☐ Friends' birthdays | THIS APP WILL RECEIVE:<br>☐ Your basic information<br>☐ Your photos<br>☑ Your birthday<br>☐ Photos shared with you<br>☑ Friends' birthdays |
| **Opt-Out (OUT)** | THIS APP WILL RECEIVE:<br>☐ Your basic information<br>☑ Your photos<br>☑ Your birthday<br>☑ Photos shared with you<br>☑ Friends' birthdays | THIS APP WILL RECEIVE:<br>☐ Your basic information<br>☑ Your photos<br>☑ Your birthday<br>☑ Photos shared with you<br>☑ Friends' birthdays |

### Recruitment and Participants

We recruited participants (N=298) through Amazon Mechanical Turk (MTurk), a recruitment source that has become popular for conducting online experiments in recent years [6]. We restricted participants to Turkers with a North American IP address and a Human Intelligence Task (HIT) approval rating of 90% or better (www.mturk.com). Participants were also required to be Facebook users and needed to be familiar with the Google Chrome browser. To motivate Turkers to complete this study, we paid $1.00 to each participant after we did a basic evaluation of the validity of task completion. Among the participants, 47% were male and 53% were female; they belonged to a wide

range of age categories (18 to 60) and covered a wide range of education levels (no high school diploma to Ph.D.).

### Measurements

*Measures for Privacy Perceptions*

To understand users' privacy perceptions, the study assessed ***perceived usefulness of the default setting*** with 3 items on a 7-point Likert scale adapted from Pu et al. [8] (α = .759). ***Perceived privacy threats of the default setting*** was measured with 3 items on a 7-point Likert scale derived from Dinev and Hart [3] (α = .866).

*Measures for Privacy Behaviors*

The following users' privacy behaviors were captured during their interaction with our manipulated app privacy notice dialogue.

***App Authorization:*** whether or not users chose to "Go to App" (1) or "Leave App" (0) during the app authorization process.

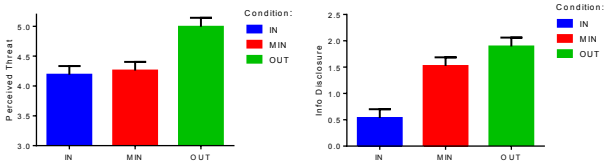
***Information Disclosure:*** The amount of information actually disclosed through the app by the user. Information disclosure was operationalized as follows:

- **0:** Did not authorize app
- **1:** Authorized app with only Basic Info
- **2 – 5:** Authorized app providing one of more of the other information attributes (Photos, Birthday, Friends' Photos, Friends' Birthday)

## DATA ANALYSIS AND RESULTS

### Effects of Default Setting

We conducted a multivariate analysis of covariance (MANCOVA) to test the effects of default setting of the privacy notice dialogue (i.e., IN, MIN, and OUT) on users' privacy perceptions and behaviors. Our results showed a significant overall main effect of default setting (Wilks' Λ = .577, $F$ (16, 609) = 9.86, $p$ < .001). Following univariate analyses of covariance (ANCOVA) uncovered how default setting affected users' privacy perceptions and behaviors specifically.




(a) (b)

**Figure 2. Effects of default setting on users' perceived threat and information disclosure**

Different levels of privacy default setting (IN vs. MIN vs. OUT) had a significant main effect on users' perceived privacy threat of those default setting ($F$ (2, 287) = 11.62, $p$ < .001). Specifically, participants in the OUT condition ($M$ = 4.991, $SE$ = .131; $p$ < .001) perceived higher privacy threat of the default setting than participants in the IN condition ($M$ = 4.258, $SE$ = .127; $p$ < .001) and the MIN condition ($M$ = 4.188, $SE$ = .128; $p$ < .001) did (Figure 2(a)).

We also found a significant main effect of the level of default setting on the amount of information users disclosed to the app ($F$ (2, 288) = 17.56, $p$ < .001). Specifically, participants in both the OUT condition and the MIN condition ($M$ = 1.89, $SE$ = .17; $M$ = 1.52, $SE$ = .16, respectively) released more information to the app than those in the IN condition did ($M$ = .54, $SE$ = .17, both $p$ < .001) (Figure 2(b)).

### Effects of App Context

MANCOVA results also showed a significant overall main effect for app context over users' privacy perceptions and behaviors (Wilks' Λ = .938, $F$ (8,281) = 2.331, $p$ = .019).

Analysis of covariance (ANCOVA) indicated that app context significantly influenced users' perceived threat ($F$ (1,288) = 4.717, $p$ = .031) and privacy usefulness ($F$ (1,288) = 4.522, $p$ = .034) of the privacy notice dialogue's default setting. To be more specific, the Birthday App triggered greater perception of the default setting being threatening ($M$ = 4.633, $SE$ = .107) and useful ($M$ = 4.729, $SE$ = .099) when compared to the Photo App ($M$ = 4.303, $SE$ = .107; $M$ = 4.430, $SE$ = .099, respectively) (Figure 3).

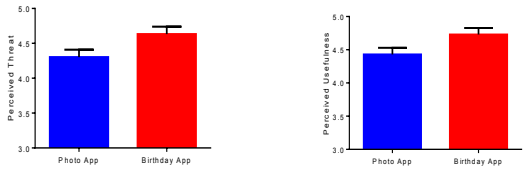



**Figure 3. Effects of app context on users' perceived threat and usefulness**

The app context also had significant main effects on users' privacy-related behaviors, including users' app authorization behaviors ($F$ (1, 288) = 8.96, $p$ = .003) and information discloser behaviors ($F$ (1, 288) = 7.38, $p$ = .007). To be more specific, we observed significant lower willingness to install the Birthday App than the Photo App and less likelihood to release information to the Birthday App than the Photo App.

### Interaction Effects between the Default Setting and App Context

Our results also indicated a significant interaction effect between these two variables on users' actual information disclosure behaviors $F$ (48, 149) = 1.52, $p$ = .03 (Figure 4).

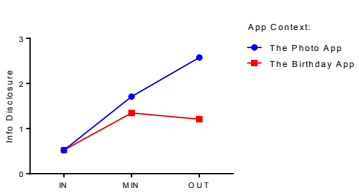



**Figure 4. Interaction effect between context and privacy default setting on users' actual information disclosure behavior**

In general, users were more likely to release their information to the Photo App than the Birthday App. For users in the Photo App conditions, the more information requested by default in the privacy notice dialogue, the more they would release their information to the app. However, for users in the Birthday App conditions, knowing that their and their friends' photos would be requested by a Birthday App scared users' away from installing the app thus preventing them to release information to the app. This finding responded to our third research question.

### Post Hoc Analysis

*Moderating Effects of Users' General Facebook Trust*

We also found one of users' individual difference variables, users' Facebook trust, played a moderating role with the privacy notice dialogue's default setting on users' information releasing behaviors.

In our analyses, we separated the pool of subjects into two groups—high Facebook trust and low Facebook trust—via a median split method, and treated general Facebook trust as a dichotomous moderator.

Our results showed that users' general Facebook trust and default setting of the privacy notice dialogue had a significant interaction effect on users' information releasing behaviors ($F$ (2,284) = 7.219, $p$ = .001) (Figure 5). In particular, among participants with higher Facebook trust, the amount of information they released to the app rose up when more information was being requested by default. For participants who did not trust Facebook much, increasing requested-by-default information from IN to MIN would lead to more information release to the app. But further increase of information inquiry from MIN to OUT not only did not evoke their information disclosure, but also prevented users from authorizing the app, which led to a decrease of the amount of information disclosed.

This interaction effect indicated that different levels of information request in the default setting of a Facebook app's privacy notice dialogue tended to have greater effects on people who trust Facebook better.

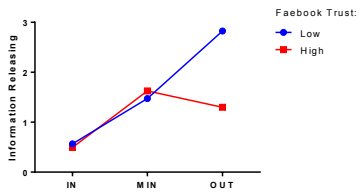



**Figure 5. Interaction effect between default settings and general Facebook trust level on users' actual information disclosure behavior**

## CONCLUSION

Our findings suggest that the amount of information requested by default and app context matter to participants. When the app asked for more than necessary information, users tended to have more negative impression over the app and deny authorizing it to keep their personal information from being released. Also, participants tended to have more concerns over releasing unnecessary photo-related information than birthday-related information.

Collectively, our findings suggest that app developers should carefully consider the relevancy of the information they request in the process of designing privacy notices. When requesting unnecessary information, app developers could harm their reputations and drive away potential users.

## REFERENCES


1. Blasiola, S. What Friends Are For: How Network Ties Enable Invasive Third Party Applications on Facebook. in *Proc. Measuring Networked Privacy Workshop at CSCW 2013*.
2. Bollen, D., Knijnenburg, B.P., Willemsen, M.C., and Graus, M., Understanding choice overload in recommender systems, in *Proc. RecSys* 2010, 63-70.
3. Dinev, T. and Hart, P., An extended privacy calculus model for e-commerce transactions. *Information Systems Research* 17,1 (2006), 61-80.
4. Facebook, Facebook Reports First Quarter 2013 Results. May 1, 2013
5. King, J., Lampinen, A., and Smolen, A. Privacy: Is There an App for That? in *Proc. SOUPS 2011 2011*.
6. Kittur, A., Chi, E.H., and Suh, B. Crowdsourcing user studies with Mechanical Turk. in *Proc. CHI 2008*, 453-456.
7. Nissenbaum, H., Privacy in Context: Technology, Policy, and the Integrity of Social Life. 2009: Stanford University Press.
8. Pu, P., Chen, L., and Hu, R. A user-centric evaluation framework for recommender systems. in *Proc. Proceedings of the fifth ACM conference on Recommender systems 2011*, 157-164.
9. Rainie, L., Smith, A., and Duggan, M., Coming and going on Facebook, 2013 11-13.
10. Smith, C., (May 2013 Update) By The Numbers: 32 Amazing Facebook Stats.
11. Steel, E. and Fowler, G., Facebook in privacy breach. http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html.
12. Wang, N., Grossklags, J., and Xu, H. An Online Experiment of Privacy Authorization Dialogues for Social Applications. in *Proc. CSCW 2013*, 261-272.
13. Wang, N., Xu, H., and Grossklags, J. Third-Party Apps on Facebook: Privacy and the Illusion of Control. in *Proc. CHIMIT 2011*.
14. Xu, H., Wang, N., and Grossklags, J. Privacy By Redesign: Alleviating Privacy Concerns For Third-Party Applications. in *Proc. ICIS 2012*.