Third-Party Apps on Facebook: Privacy and the Illusion of Control

Na Wang
The Pennsylvania State University
University Park, PA 16802
nzw109@ist.psu.edu

Heng Xu
The Pennsylvania State University
University Park, PA 16802
hxu@ist.psu.edu

Jens Grossklags
The Pennsylvania State University
University Park, PA 16802
jensg@ist.psu.edu

ABSTRACT
Little research examines the privacy threats associated with the use of third-party apps on Facebook. To address this gap in the literature, we systematically study third-party apps' current practices for privacy notice and consent by: i) collecting data from the 1800 most popular Facebook apps to record their data collection practices concerning users and their friends, and ii) developing our own Facebook app to conduct a number of tests to identify problems that exist in the current design of authentication dialogs for third-party apps on Facebook. To address these problems, we propose two new interface designs for third-party apps' authentication dialogs to: i) increase user control of apps' data access and restrict apps' publishing ability during the process of adding them to users' profiles, and ii) alert users when their global privacy settings on Facebook are violated by apps. This research provides both conceptual and empirical insights in terms of design recommendations to address privacy concerns toward third-party apps on Facebook.

Categories and Subject Descriptors
D.4.6 Security and protection, H.5.2 User Interfaces

General Terms
Design, Security, Human Factors.

Keywords
Privacy, Third-Party Applications (Apps), Control, and Online Social Networks, Notice and Consent.

1. INTRODUCTION
In recent years, Online Social Networks (OSNs) have moved from being a niche phenomenon to mass adoption. Facebook, for example, has transformed from a localized college network website to one of the most popular OSNs with more than 750 million active users around the world [1]. There is now sufficient evidence showing that Facebook gradually expands into a ubiquitous giant information repository which documents users' personal data and logs users' interaction information with their friends and various objects (i.e., pages, groups, events, and community pages).

ACM CHIMIT '11, December 4, 2011, Boston, MA, USA.

According to publicly available information, Facebook users share more than 30 billion pieces of content (e.g., web links, news stories, blog posts, notes, photo albums), and interact with over 900 million objects each month [1]. These high-volume information exchange activities introduce a variety of privacy risks for Facebook users. As identified by prior privacy research, these may include, but are not limited to, accidental information disclosure, damaged reputation and image, unwanted stalking, and reconstruction of users' identities [6, 7, 10, 13].

Adding to these concerns, a Wall Street Journal (WSJ) study found numerous third-party applications (apps) on Facebook extracting identifiable user information from the platform and sharing this bounty with advertising companies [20]. Thus, an additional dimension that represents the complexity of studying privacy risks on Facebook is introduced by the large amount of information interaction between third-party developers and Facebook users.

To the best of our knowledge, there is little research on addressing the privacy threats associated with the use of Facebook third-party apps. In addition to the WSJ article, Besmer and Lipford examined users' motivations, intentions, and concerns with using applications, as well as their perceptions of data sharing. Their results indicate that Facebook users are not truly understanding and consenting to the risks of apps maliciously harvesting profile information [4]. Similarly, King and her colleagues also studied users' misunderstandings and confusion concerning apps' functionality and information practices [17]. Taking an engineering view, Hull *et al.* suggest visualization enhancements of the third-party apps' information accessing and publishing practices [15]. In doing so, users might have a better awareness how the app will use their information and thus users might be able to avoid some undesirable information leakage.

Regarding generic Facebook privacy settings, Lipford *et al.* designed an interface with a better audience view [18]. In critiquing Facebook's available privacy control options, they identified some design flaws that might lead to users' misunderstandings. In another study, Shehab and his coauthors developed a Firefox browser extension that allows users to configure their privacy settings at the time when they installed the apps and provides recommendations on requested information [19].

However, previous research does not examine the circumstances under which users' global privacy settings are potentially violated by third-party apps. Related work does also not address how to improve the notice and consent mechanism to more effectively alert users when such violations happen, and when more attention should be invested by the user.

More specifically, to address these concerns, we aim to provide Facebook users with: 1) better control options to limit third-party apps' data read, write and page manage abilities on Facebook, and 2) better warning mechanisms to inform users under such circumstances when their privacy settings are violated by third-party apps.

To achieve these goals, we first examine the current implementation of user information control on Facebook (e.g., how to limit their information sharing with other users and third-party apps), followed by analyzing patterns of personal information transmission from users to third-party apps. Our results confirm that there is a large amount of users' personal information transmitting from Facebook to external entities. We further investigate information transmission using actual field data from the 1800 most popular third-party apps on Facebook. Our results provide a preliminary but detailed picture of personal information transmission in the wild, rather than as discerned through surveys and laboratory experiments. We also develop our own Facebook app to conduct a series of tests for the purpose of observing third-party apps' practices for privacy notice and consent. Based on these insights learned from our tests, we point out several flaws that exist in the current design of authentication dialogs for third-party apps. In hoping to address these problems, we propose and evaluate two new interfaces for the authentication dialog to help users better manage their personal information transmission on Facebook. The paper concludes with a discussion of theoretical and design implications, and directions for future research.

2. OVERVIEW OF PRIVACY CONTROL OPTIONS ON FACEBOOK

2.1 Information Control among Users

Users can adjust their privacy settings to set limits for other users' ability to access uploaded and created content. By adjusting these settings, Facebook users can: 1) control basic information their friends will use to find them on Facebook; 2) control who can see what they share; and 3) edit lists of blocked people. **Figure 1** shows the interface of the global privacy settings.

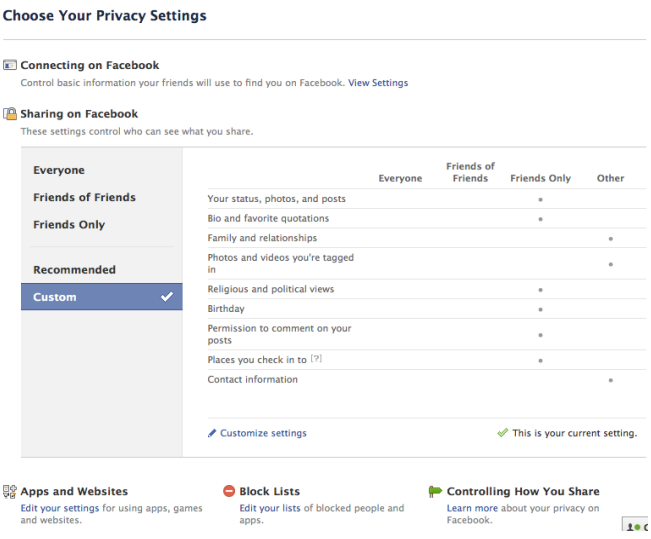

Figure 1. User Interface of Privacy Settings on Facebook as of 5/10/2011.

2.2 Information Control between Users and Third-Parties

In addition to provisions to limit information access among users, Facebook also provides mechanisms to restrict information transmission between users and third-party apps, even though these mechanisms are found to be problematic later in our study.

To limit third-party apps' information access, Facebook primarily relies on the OAuth 2.0 protocol which is used for third-party authentication and authorization. In the traditional client-server authentication model, the client can access a protected resource on the server by authenticating with the server using the resource owner's credentials. OAuth 2.0 adds an authorization layer and separates the role of the client (third-party application) from that of the resource owner (Facebook user) [14]. **Figure 2** demonstrates the flow of the OAuth 2.0 protocol.

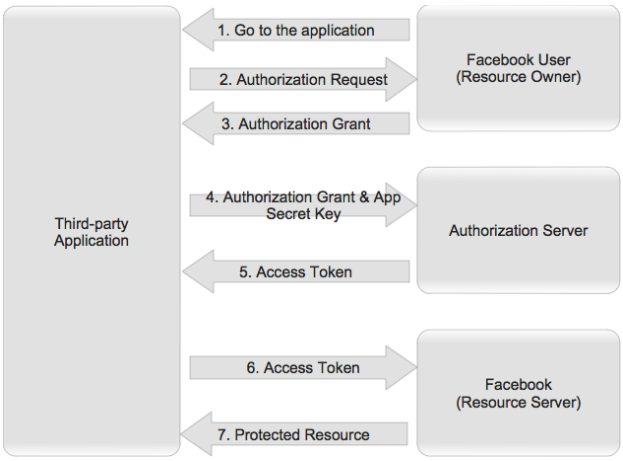

Figure 2. The OAuth 2.0 protocol as of 5/10/2011.

2.2.1 Authentication before Installing Apps

Under the OAuth 2.0 protocol, when a user wants to add an application to her Facebook profile, the application is required to ask the user for her authorization to access, for example, basic information and/or other shared data on Facebook. **Figure 3** includes a representative example of the user interface associated with this privacy authentication dialogue.

In the sample authentication dialog shown in **Figure 3**, the first category "access my basic information" represents the default information that will be accessed by the app, which includes user's basic information such as name, profile picture, gender, network, user ID, list of friends, and any other information the user has shared with everyone. If the app developer anticipates a need for information beyond these basic categories, she will need to request extended permission(s) from the user. As shown in **Figure 3**, in addition to the category of "basic information", the apps could request extended permissions to access more data (e.g., contact information, photos, videos and friends' information, etc.) or to act on behalf of the user (e.g., to post on users' wall, and send text messages to users).[1]

[1] There are a total of 60 extended permissions for additional reading, writing, and page management operations (as of 5/10/2011). See URL: http://developers.facebook.com/docs/authentication/permissions.

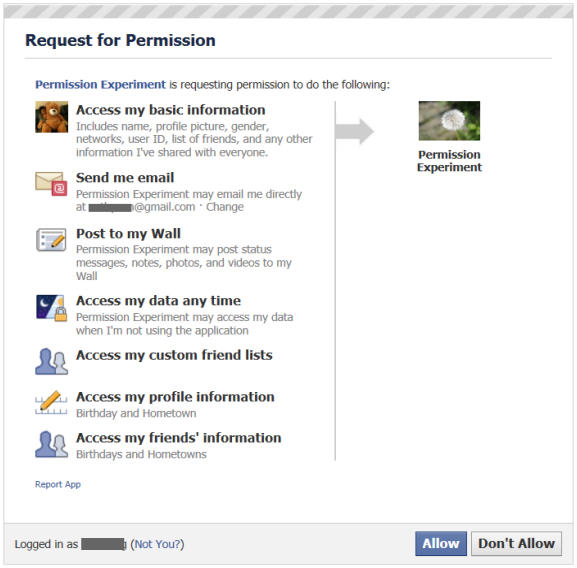

Figure 3. Current Third-Party Apps' Authentication Dialog as of 5/10/2011.

2.2.2 Information Control after Installing Apps

In the Facebook privacy settings, there is a section called "Apps and Websites" which enables users to control certain aspects of the information sharing between them and previously installed apps. As shown in **Figure 4**, users could remove some information categories from this list, which would make that type of information no longer available to the app. There are, however, four categories of information that cannot be removed (i.e., "Send me email", "Access my profile information", "Access my friends' information", and "Access my photos and videos").

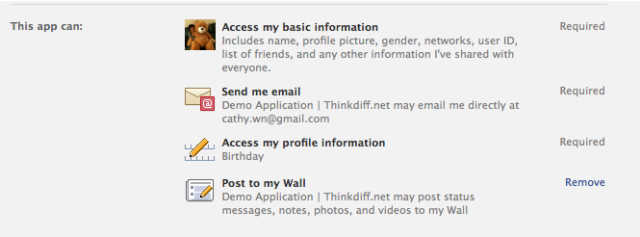

Figure 4. Post-Installation Privacy Settings for Apps as of 5/10/2011.

3. THIRD-PARTY APPS' DATA COLLECTION PRACTICES

In this section, we discuss the scope of user information that apps could potentially collect from users of the Facebook platform and transmit to advertising companies or other third parties. Field data from the most popular 1800 third-party apps on Facebook was collected in December 2010 and analyzed to investigate third-party apps' data collection practices.

From the Facebook application directory[2], we locate the URLs for the most popular 1800 applications in nine categories. These nine categories are business, education, entertainment, friends & family, games, just for fun, lifestyle, sports, and utilities. We collected data from the top 200 most popular applications from each category. By going through the list of these applications, we recorded the profile page URL for each application. Then, we used the software "Locoyspider" to collect and save data from these profile pages, as well as record the number of monthly active users for these applications. Next, we used the list of "Go to App" URLs to either access the authentication dialog ("Request for Permission") which lists all the information that the app requests from users, or to be redirected to the app's external page. In our dataset, we only consider those applications which would pop-up the privacy authentication dialog after clicking the button of "Go to App". From these authentication dialogs, we capture the types of information each app desires to access from users. Combining this information (i.e., types of information requests) with the number of monthly active users for each application, we can count how many times a specific type of information is released to an app within a month.

Among those 1800 most popular applications, there were 1305 applications displaying authentication dialogs when they requested data access from users. From the end user's perspective, there were 12 categories of information/behavior requested by the authentication dialogs. For each category of these requests, we first compiled a list of applications that require it. We summed up the number of monthly active users for each application on the list to get the total number of users who were requested for this type of information. We treat this total number as the total times that such user information is requested per month (see **Table 1**).

Table 1. Authorization Requests Presented to the User.

Data Category/ Access Category	Number of apps requesting category (percentage of apps requesting category)	Total times a category is requested by apps
Access my basic information	1305 (100%)	857,821,274
Send me email	454 (34.79%)	238,991,048
Post to my wall	670 (51.34%)	137,473,280
Access my profile information*	148 (11.34%)	178,912,316
Access my data any time	76 (5.82%)	17,450,664
Manage my pages	8 (0.61%)	237,067
Access my photos and videos	128 (9.81%)	43,227,008
Access my friends' information	148 (11.34%)	68,436,680
Access posts in my News Feed	66 (5.06%)	30,635,352
Online Presence	16 (1.23%)	4,003,824
Access my family & relationship	28 (2.15%)	6,617,296
Access Facebook Chat	8 (0.61%)	1,739,160
Send me SMS messages	10 (0.77%)	1,195,720

* User information accessed by this category may vary based on different app requests.

[2] See URL: https://www.facebook.com/directory/applications/.

As shown in **Table 1,** more than 850 million times users were asked to release their basic information to applications. Further, the top three most frequently requested extended permissions are: "Send me email", "Access my profile information", and "Post to my Wall".

4. THIRD-PARTY APPS' PRACTICES FOR PRIVACY NOTICE AND CONSENT

To examine the current privacy notice and consent practices by third-party apps on Facebook, we developed our own Facebook app "Permission Experiment" and performed a series of tests to address the following two questions:

Question 1 (Q1): *To which extent could third-party apps override users' global privacy settings on Facebook?*

Question 2 (Q2): *To which extent does the authentication dialog truly reflect the third-party apps' information practices?*

We present our findings in the sub-sections below.

4.1 Tests of Privacy Violations (Q1)

4.1.1 A Case of "Happy Calendar 2011"

User A prefers to block disclosure of her birthday. Accordingly, her privacy setting for this information category is "Only me", which means her birthday cannot be seen by other users on Facebook except herself. When this user adds the app "Happy Calendar 2011" to her profile, she is asked to grant the app permissions to access her and her friends' birthdays and to publish them. Like most users, *User A* immediately grants the app all requested permissions. Later, *User A* finds out that "Happy Calendar 2011" created an album in her profile and posted all her friends' birthdays that she can access, as well as her own, in a calendar image with their profile pictures being visible in the corresponding date fields (see **Figure 5**). Moreover, *User A*'s friends received a wall post notifying them of the creation of this album and how they can access it. As a result, the "birthday", which *User A* intended to keep private, is now accessible by her friends. We consider this case as a privacy violation in which the third-party app overrides users' global privacy settings.

Figure 5. A Case of Privacy Breach by Third-Party Apps.

4.1.2 Further Tests of Privacy Violations

In the above case, we used "birthday" as a representative type of personal information to supply an example of third-party apps overriding users' privacy settings. We further utilized our own app "Permission Experiment" to run several similar tests for other types of information. Our results indicate that the privacy breach demonstrated in the case of "Happy Calendar 2011" is generalizable to many different types of information requests. As long as a user grants the app the permission to access her own and her friends' data, in conjunction with a publishing permission, then user's profile information like "birthday" but also other contents (e.g., photos, videos, comments, and everything she shared), could be accessed and released by that app. Thus, we conclude with respect to *Q1* that privacy violations may exist when there is conflict between users' privacy settings and apps' data collection and publishing practices. Our tests confirm that Facebook's powerful API enables application developers to collect and publish user data in an aggressive fashion.

4.2 Tests of Reflection (Q2)

Question 2 asks about the extent to which the authentication dialog truly reflects the third-party apps' information practices. To address this question, we use our app "Permission Experiment" to request different extended permissions from a hypothetical user account (*User A*) and examine the scope of information that can be accessed when the permission is being granted. The following procedures state the process of our tests:

Step 1. Different extended permissions were added to the source code of our app "Permission Experiment" for requesting extended permissions from *User A*.

Step 2. Observe how the authentication dialog changed correspondingly.

Step 3. The app "Permission Experiment" was added to the user's profile.

Step 4. Referred to the Facebook developer's documentation to carefully examine these extended permissions, e.g., what kind of user information can be accessed by the app.

Step 5. Went to *User A*'s "Apps and Websites" settings to observe which extended permission(s) can be removed.

Next, we discuss our findings.

4.2.1 Chaotic Display

When developers change the source code to request different permissions for accessing users' personal information or publishing rights, the authentication dialog will change, however, the display can be chaotic. For example, when the app is asking to access photos and videos uploaded by the user's friends as well as those photos and videos friends were tagged in, the display of these two groups of permissions would look confusing, as highlighted in **Figure 6**.

Regarding the phrase of "Photos, Videos and Photos and Videos of Them" marked by the red line in **Figure 6**, we anticipate users to experience confusion concerning its implications. Further, the somewhat awkward treatment of English grammar does very likely reduce users' understanding. Thus, it might be very difficult for them to understand the meaning and implication of these extended permissions.

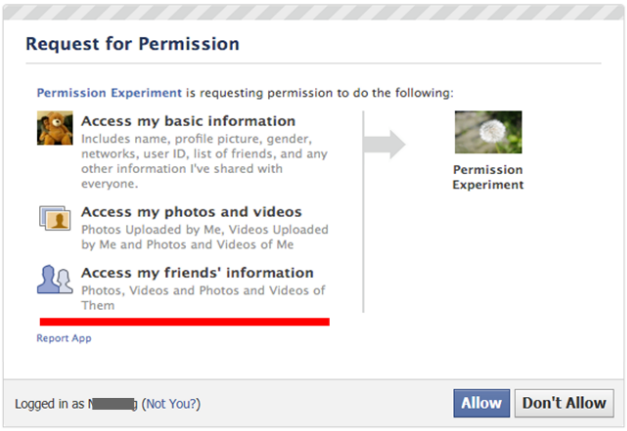

Figure 6. Chaotic Display of Extended Permissions (Marked in Red) as of 5/10/2011.

4.2.2 Insufficient Reflection

To further address our second question (Q2), we use a simple case of "Access my photos" to demonstrate whether the authentication dialog will truly reflect the third-party apps' information practices. When our app "Permission Experiment" requests an extended permission to access user photos ("user_photos"), users will see a corresponding authentication dialog (as shown in **Figure 7**) when they add the app.

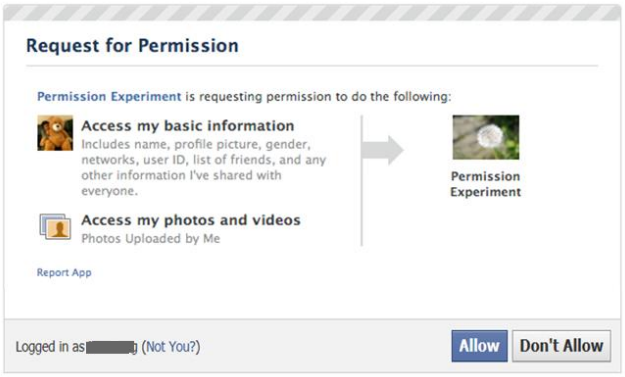

Figure 7. The Authentication Dialog for the Extended Permission "user_photos" as of 5/10/2011.

In this dialog window, the extended permission asking for access to user photos is explained as data access request for "Photos uploaded by me". This explanation is confusing because users might easily entertain the belief that only the photos they have shared on Facebook would be accessed by that app.

However, in fact, with this simple "user_photos" permission being granted, the real amount of information that the app could access is far more substantial and exceeds the shared photos themselves. More specifically, the "user_photos" permission actually enables the app to access all albums objects the user has created. For each album object, it has ten properties and three connected objects (photo, comment, and picture) which do not require any permission. And within those three connected objects, both photo and comment have their own properties and further connected objects, which distribute this permission further. In **Figure 8**, we demonstrate the scope of accessible information after granting permission.

Based on our case analysis of "Access my photos", we conclude that the prompting messages displayed in the authentication dialog fail in informing users about the actual scope of personal information that will be accessed by the app. If one app asks for extended permissions to access a certain object, with that permission being granted, the app can access not only all of its non-permission required properties but also its connected objects' properties.[3] Furthermore, if the second-level objects are connected to some third-level objects that are not included in the permission request, those third-level objects' properties will be available to the app. And this information access chain will not stop until it reaches an object that does not have any further object connecting to it.

4.2.3 Limited Control

In the current design of the authentication dialog, we found that there is no way for users to limit the apps' information access or publishing abilities during the installation process. Even the post installation information settings cannot sufficiently help users to control what information they share with apps. In "Settings for Websites and Apps", users could only remove some categories of the extended permission(s). But users have no control options for those extended permissions marked as "required" (see **Figure 4**).

Surprisingly, even developers cannot define removable or required extended permissions. In our tests, without any specific definition in our source code, when we asked for different extended permissions, some of these were marked as required and thus cannot be removed from the "Settings for Websites and Apps". In contrast, other extended permissions were available for removal by users. So far, we have not found the patterns regarding when and what extended permissions could be removed by users.

5. PROPOSED NEW DESIGNS

5.1 Design Principles

Our analyses and tests of third-party apps' current practices for privacy notice and consent have identified a number of problems that exist in the current design of the authentication dialogs. Although, we are aware of the fact that there is no panacea for privacy settings, there is room for serious improvement. Our results suggest a number of heuristics to improve the design and the effectiveness of privacy notice and consent:

Known information – The authentication dialog should provide explicit signals for users to distinguish what data would be accessed by the app and how the data would be used.

Control before allowing – The authentication dialog should provide options for users to control the app's data reading and writing practices before adding the app to their profiles.

[3] "Non-permission required properties" can be fetched without any extended permission (e.g., all properties related to comments on Facebook, including id, from, message, created time, likes, user likes and type). To be more specific, if a user grants an app access to her photos, then this app can also access all the comments posted under this user's photos.

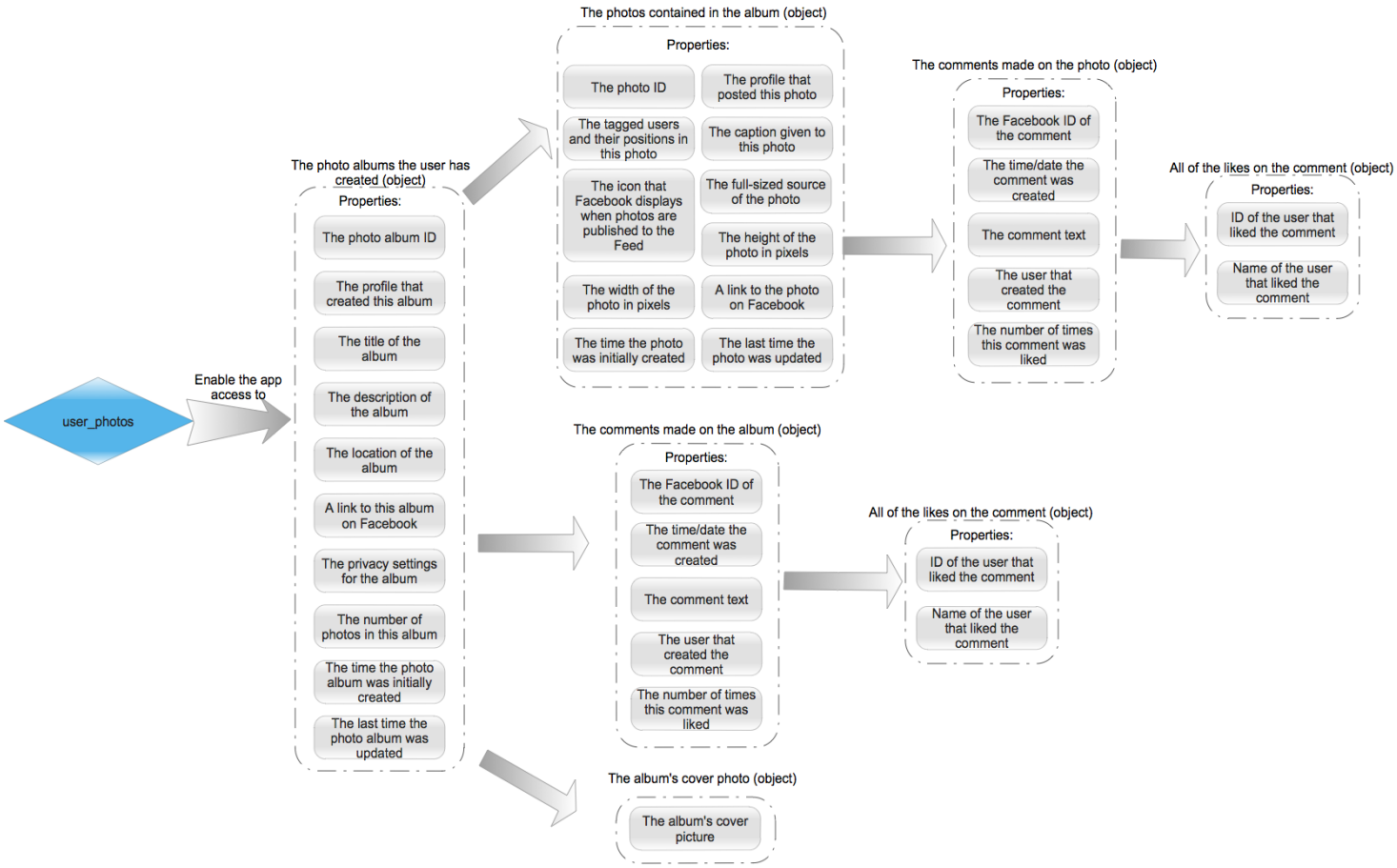

Figure 8. The Real Amount of Information Could Be Released After Granting Permission "user_photos**" as of 5/10/2011.**

Conflict caution – The authentication dialog should provide warning signals to the users when data and publishing permissions requested by the app will violate their global privacy settings.

Privacy indication – The authentication dialog should reflect a user's current privacy settings.

The first three design principles were developed to address the identified flaws that exist in current designs of authentication dialogs. The fourth design principle was developed to test whether users want the authentication dialog to further reflect their privacy settings. In order to better isolate the implications of the fourth design principle, we split our analysis by providing two new designs addressing different aspects of our suggestions.

5.2 Alternative Interfaces

Kelley *et al.* developed a privacy "nutrition label" that presents to consumers the ways organizations collect, use, and share personal information [16]. Their design, inspired by the field of the nutrition warnings and advice, aims to: 1) clearly highlight the meaning of different labels so that users can easily understand the different sets of information; 2) use different font highlights to separate sets of information in order to expedite the users' navigation through the list; and 3) have a bold and clear title to inform the user of the purpose of the information in each section [2, 3, 8, 11]. In this research, we aim to include similar design elements in our designs.

As Carroll highlighted in his book [9], "people rely on analogies with familiar, readily envisaged domains to build mental models of less-familiar, less-visible domains". Following this design guideline, we have adopted icons and color themes that are well consistent with users' mental models in their familiar and readily envisaged domains. For instance, as a sign for alert in our daily life, we have used the red exclamation mark to indicate the conflict between users' privacy settings and apps' requests for data access.

Envisioned by the proposed design heuristics and previous analyses, we now present our alternative interfaces for privacy authentication dialogs by third-party apps on Facebook.

5.2.1 Monochrome Authentication Dialog (MONO)

The *MONO* interface design of the authentication dialog aims to fulfill the first three design principles (see **Figure 9**).

Below we describe our major design elements.

The Layout of Permissions: All types of data (basic information and data reading permissions) required by the app are listed in the first column. The first row displays the information regarding how the app will use the data (including data writing and page management permissions).

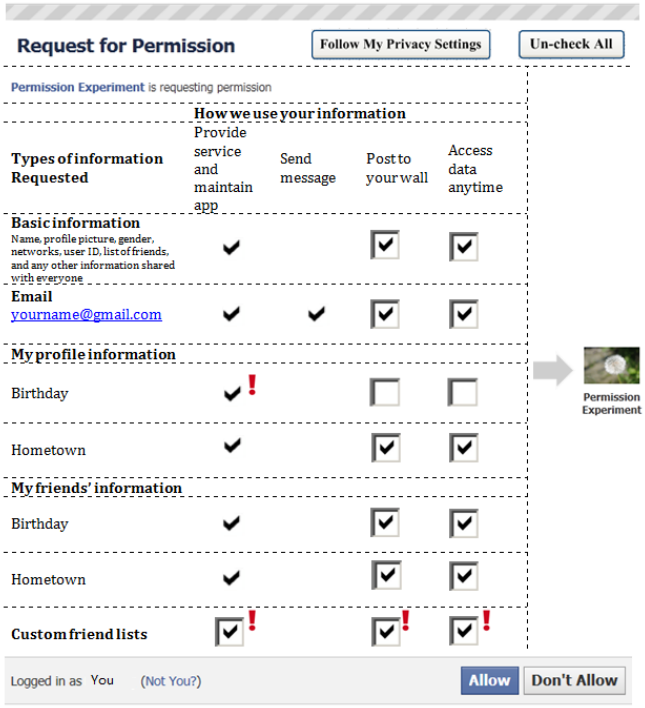

Figure 9. Proposed *MONO* Interface Design.

The Tick Mark and Checkbox: *Un-clickable tick marks* represent those types of information that will be accessed and used by the app. Users have to give out corresponding information to use the app. The *checked* check box means that users will allow the app to access and use certain information. The *un-checked* check box means that users will not allow the app to access or use the corresponding information.

The Red Exclamation Point: When the information requested by the app conflicts with the user's privacy settings, the red exclamation point alerts users about the potential conflict.

Shortcut Buttons: We add two buttons to help users control how the app accesses and publishes their information. When clicking *'Follow My Privacy Settings'*, those check boxes with the red exclamation point alert will be unchecked. Under this situation, the app will not be allowed to use these specific types of information. When clicking *'Uncheck All'*, all the check boxes will be unchecked, i.e., only required types of information will be shared.

5.2.2 Polychrome Authentication Dialog (POLY)

Our second design of the authentication dialog, the POLY design, is an enhanced version of the MONO design, with a three-color scheme to reflect users' privacy settings, which addresses the fourth design principle (see **Figure 10**).

GREEN indicates the current privacy setting for the corresponding information is "Everyone" and it will NOT be violated by adding the app to the user's Facebook account.

RED indicates the current privacy setting for that information is "Only Me" or "Specific People…" and it will be violated by adding the app to the user's Facebook account.

YELLOW indicates the current privacy setting for that information is something beyond "Everyone", "Specific People…", or "Only Me". For example, if a user's privacy setting for "Birthday" is "Friends Only" or "Friends of Friends", then in the authentication dialog, the background of the checkboxes in the "Birthday" row will be marked yellow. In this case, the app would be able to access this personal information item while other users may have partially restricted access. Even though the original user's privacy setting is not directly violated by the app, there might be some potential privacy risks for the user to allow the app to access these data.

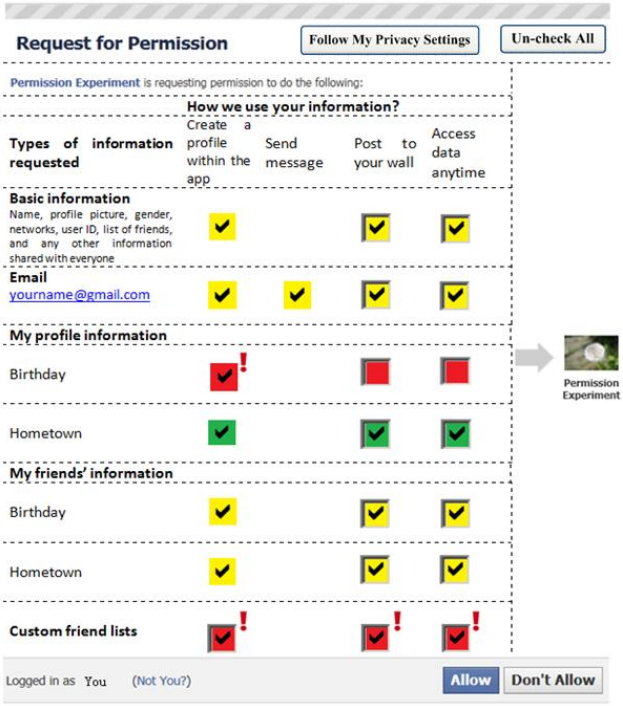

Figure 10. Proposed *POLY* Interface Design.

6. PRELIMINARY USER EVALUATION

To gain a preliminary understanding of user feedback, we conducted a qualitative study to evaluate the MONO and POLY designs. The intent of this evaluation approach is to ensure that the design principles identified in the conceptual analysis are adequately met in the opinion of the target user population. We considered protecting one's privacy as a sensitive topic; there may be social implications to responses people give. When collecting data about sensitive topics, it is appropriate to utilize open ended questions to permit respondents expressing themselves in a way that they do not feel threatened, and allowing them to say as much or as little as they would like and not be confined to a limited set of answers that are available in a Likert-type survey design.

6.1 Participants and Procedure

Participants were recruited from junior/senior levels of undergraduate classes at a public university in the United States. We specified that participants must be active Facebook users. Two extra credit points were awarded for their participation in this study. There were in total eleven participants who consented to partake in our user study. Among these eleven participants, two were female and nine were male; and they identified their ages as 20 to 24.

Participants were first asked to review the third-party apps they added to their Facebook accounts and recall their installation and user experience, followed by the introduction of our proposed MONO and POLY designs. The next series of questions was aimed at evaluating our new designs. Participants were asked to respond to open-ended questions about their attitudes toward our proposed MONO and POLY designs, e.g., whether they want the authentication dialog to reflect their privacy settings on Facebook, and to what extent our POLY design could reflect their privacy settings. Finally, participants were asked to compare and contrast three types of authentication dialog designs: the current one on Facebook, the MONO design, and the POLY design.

6.2 Data Analysis and Results

The data collected was coded based on a set of rules developed from the questions asked, as well as information received from the question responses. As the first step, we examined participants' responses to the open-ended questions and identified significant concepts and aspects through content analysis of their answers. We then applied a more thorough process to code their answers for in-depth analysis. In this procedure, we examined the patterns in subjects' responses and attempted to correlate concepts generated in the coding process. By doing this, we expected to find out participants' attitudes and preferences on the current Facebook apps' authentication dialogs and our newly proposed MONO and POLY designs. More importantly, we expected these results could infer a better authentication dialog design in practice.

6.2.1 General Attitudes toward New Designs

The advantages of our new designs in terms of providing users with better control options to limit apps' information activities and better warning mechanisms to inform them about privacy violations have been confirmed by participants. All participants highlighted the importance of improving current privacy authentication dialogs on Facebook. For example, participants commented the following:

"[T]he proposed designs are vastly superior to the current design."

"Both the MONO and POLY dialog screens are effective ways of allowing users to see and change application requests for information."

"Both designs address basic issues such as notifying whether or not the third-party app will violate previously established privacy settings. They do an excellent job informing the user about the consequences of using the application."

When asked whether they want the authentication dialog to reflect their Facebook privacy settings, all participants responded positively. They would like the authentication dialog to reflect their privacy settings *"because it will help them manage their privacy and security" and "forces [them] to be more aware of their privacy settings"*. They also believe the reflection of their privacy settings on the authentication page could help them to avoid possible violations caused by third-party apps:

"This allows me to view when there may be a potential conflict with my already established privacy settings."

One participant even hoped to have every detail of his privacy setting to be reflected in the authentication dialog. In addition, one participant questioned the effectiveness of POLY design in the situation where a user's privacy settings were too strict to be reflected by the POLY interface.

Interestingly, the participants also mentioned other perspectives which were out of scope of our design considerations:

Friends' Information

Four participants mentioned the ability for an application to gather information about one's friends should be another issue to be addressed. This is because *"[the user's] friends never download or agreed to the application's term"*, and the user *"does not own [his or her] friends' information"*. If the user is not diligent about setting secure privacy settings, the apps may be able to access his/her friends' information. This is especially unfair for his/her friends who may be proactive and try to make smart privacy choices.

Transparency of Information Flow

One participant advocated for the idea that "*the information extracted from a user's profile should be monitored"* in a real time fashion. In this way, the user could quickly access when and what information was accessed and used by the apps. One participant also suggested the authentication dialog to inform the user *"why the app need the information they take"*.

6.2.2 Comparing Two Designs

We asked participants to compare and contrast three types of authentication dialog designs: 1) the current one on Facebook, 2) the MONO design, and 3) the POLY design. Based on our data coding, we developed four comparison themes in Table 2.

Table 2. Comparing Two Designs.

Comparing Themes	**Authentication Dialog Designs**
Visual Effects	Ability to grab users' attention.
Perceived information control ability	Participants' perceived effectiveness of authentication dialogs in helping users better control the app's information accessing and publishing practices.
Perceived effectiveness in alerting potential privacy violations	Participants' perceived effectiveness of authentication dialogs in alerting users about potential privacy violations.
Overall likability	The extent to which a person likes the design of the authentication dialog.

Visual Effects

All participants highlighted that both MONO and POLY were good at grabbing users' attention. Three participants thought the new design with the exclamation point in red were attention grabbing. They believed that with the implementation of the new designs on Facebook, users would definitely pay more attention to privacy and security issues.

One participant thought that the introduction of the color in POLY was too distracting for users. However, the majority of participants believed that the POLY design did a better job than the MONO design: *"with the bright colors displayed on the request for permission page, it can't help but draw attention."*

Perceived Information Control Ability

The majority of the participants believed that the new designs could help them to better control the app's information accessing and publishing practices. They thought the new design elements

would place control in the hands of users. Only one participant doubted whether the new interface offered a sufficient degree of control. Nevertheless, the respondent affirmed the added convenience and potential to raise awareness.

Perceived Effectiveness in Alerting Privacy Violations

Participants regarded the new POLY design as superior in terms of alerting potential privacy violations, due to its use of the three-color scheme reflecting the user's privacy setting and alerting users about potential privacy violations:

"[T]he POLY design is colorful, it would make users more aware of the [privacy] settings."

"[T]he POLY design integrates a color scheme that provides even more awareness of when apps are conflicting with personal privacy settings."

As the POLY design could indicate how private the information was considered by the user when the app asked access permission to it, it was much easier for conflicts to stand out in the POLY design than it was in the MONO design. Both the exclamation mark and the red color, as the universal signals for danger and problem, can help users be aware of the item when a conflict materializes. Contrarily, the design in the current authentication dialog has no alert information when a user's privacy settings conflict with an app's information accessing or publishing practices.

In addition, participants also mentioned that both the MONO and POLY designs would be useful as long as the users would take the time to learn the new interface and pay attention to the signals. One participant commented that without educating and teaching users about what was happening to their personal information, none of the new design would work.

Overall likability

Six out of eleven participants liked the POLY design better due to the implementation of the color scheme that reflected users' privacy settings. As suggested by these participants, the POLY design was more eye-catching because the three-color scheme could better inform users about the potential privacy violations. When something was highlighted in red, the user would relate it either as a bad thing or as a stop sign. This would make users think twice or at least try to read and understand how much information they may allow third-party apps to access.

On the contrary, four participants believed that the MONO design was more aesthetically pleasing and easier to understand. They considered the three-color scheme of the POLY design *"will distract users"* and *"it would be overwhelming for users to view"*.

7. DISCUSSION AND CONCLUSION

This research identifies a number of challenges at the interface between the representation of material terms to users and the underlying data collection and transmission practices by apps:

- During the process of adding an app to their profiles, users do not have any control to limit the app's access to their personal information or restrict the app's publishing practices. Only after adding the app, users can edit some categories of information access or publishing practices via adjusting their "Apps and Websites Settings" under their privacy settings.

- Facebook's powerful APIs could enable third-party apps to override users' privacy preferences expressed through their privacy settings.

To address these problems, we propose two new interfaces of the third-party app's authentication dialogs to: i) empower users to control and limit apps' information access and to restrict apps' publishing ability during the process of adding the apps to the user profile, ii) alert users when their global privacy settings on Facebook are violated by the apps, and iii) help users better understand what kinds of their personal information will be accessed and used by the app.

A preliminary user study with eleven participants was conducted to evaluate the authentication dialogs we proposed. Based on the analysis of participants' responses, we have gained insightful lessons on the design of third-party apps' authentication dialogs on Facebook. First, a well-designed authentication dialog should stand out to be noticed. Users will be aware of the conflicts between their privacy settings and third-party apps' information accessing and publishing practices only if they pay attention to the design cues spontaneously. Second, a well-designed authentication dialog should do a better job in both warning users of the potential privacy conflict and providing users with options or suggestions to avoid such conflict. Third, the authentication dialog should be easy for users to understand and be consistent [12].

Finally, although all participants wanted the authentication dialog designed to reflect their global privacy settings on Facebook, the use of a color scheme was not always the favored solution. Some participants argued that the use of the three-color scheme was eye-catching; and thus they regarded it as an advantage. On the contrary, other participants regarded it as a disadvantage because they considered it as a distraction. Based on these results, it seems fair to conclude that the three-color scheme implemented in POLY design is not a perfect way to reflect users' privacy settings. In our future work, we aim to further improve our solution to achieve a superior notice and consent experience.

In summary, this research seeks to add to the research literature by providing a greater understanding of privacy issues regarding third-party apps on Facebook. The development of design principles as well as the preliminary evaluation of our proposed new designs could potentially alleviate users' privacy concerns without sacrificing their social and entertainment needs pertaining to third-party apps. Moreover, our work offers practitioners (such as application developers and social networking service providers) wake-up calls and suggestions for further improvements. In future work, we will implement our new designs as working interfaces and embed them during controlled experiments into the Facebook environment [5]. We are particularly interested in large-scale studies to study to what extent users understand and share when interacting with third-party apps on Online Social Networks.

8. ACKNOWLEDGMENTS

The authors gratefully acknowledge the financial support of the National Science Foundation under grant CNS-0953749. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

9. REFERENCES

[1] Facebook Statistics. 2010; Available from: http://www.facebook.com/press/info.php?statistics.

[2] Administration, U.S.F.a.D. Guide to nutrition labeling and education act requirements. 1994; Available from: http://www.fda.gov/ora/inspect_ref/igs/nleatxt.html.

[3] Belser, B., Designing the food label: nutrition facts. AIGA Journal, 1994.

[4] Besmer, A. and H. Lipford. Users' (mis)conceptions of social applications, *Proceedings of Graphics Interface (GI'10)*, Ottawa, Canada, May/June 2010, p. 63-70.

[5] Böhme, R. and S. Köpsell. Trained to accept?: A field experiment on consent dialogs, *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI'10)*, Atlanta, GA, April 2010, p. 2403-2406.

[6] boyd, d. and N. Ellison, Social network sites: Definition, history, and scholarship. Journal of Computer Mediated Communication, 2008. 13(1): p. 210-230.

[7] Brandimarte, L., A. Acquisti, and G. Loewenstein. Misplaced confidences: Privacy and the control paradox, *Workshop on the Economics of Information Security (WEIS)*, Boston, MA, June 2010.

[8] Buckley, P. and R. Shepherd, Ergonomic factors: The clarity of food labels. British Food Journal, 1993. 95(8): p. 18-21.

[9] Carroll, J.M., HCI models, theories, and frameworks: Toward a multidisciplinary science. 2003: Morgan Kaufmann Pub.

[10] Debatin, B., J. Lovejoy, A. Horn, and B. Hughes, Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of Computer Mediated Communication, 2009. 15(1): p. 83-108.

[11] Golan, E., F. Kuchler, L. Mitchell, C. Greene, and A. Jessup, Economics of food labeling. Journal of Consumer Policy, 2001. 24(2): p. 117-184.

[12] Good, N., J. Grossklags, D. Mulligan, and J. Konstan. Noticing notice: A large-scale experiment on the timing of software license agreements, *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI'07)*, San Jose, CA, April /May 2007, p. 607-616.

[13] Gross, R. and A. Acquisti. Information revelation and privacy in online social networks, *Proceedings of the ACM Workshop on Privacy in the Electronic Society (WPES)*. Alexandria, VA, November 2005, p. 71-80.

[14] Hammer-Lahav, E., D. Recordon, and D. Hardt (2011) The OAuth 2.0 authorization protocol draft-ietf-oauth-v2-12.

[15] Hull, G., H. Lipford, and C. Latulipe, Contextual gaps: Privacy issues on Facebook. Ethics and Information Technology, 2010.

[16] Kelley, P., J. Bresee, L. Cranor, and R. Reeder. A nutrition label for privacy, *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS)*, Mountain View, CA, July 2009.

[17] King, J., A. Lampinen, and A. Smolen. Privacy: Is there an app for that?, *Proceedings of the 7th Symposium On Usable Privacy and Security (SOUPS)*, Pittsburgh, PA, July 2011.

[18] Lipford, H., A. Besmer, and J. Watson. Understanding privacy settings in Facebook with an audience view, *Proceedings of the USENIX Workshop on Usability, Psychology and Security*, San Francisco, CA, April 2008, p. 1-8.

[19] Shehab, M., S. Marouf, and C. Hudel. ROAuth: Recommendation based open authorization, *Proceedings of the 7th Symposium On Usable Privacy and Security (SOUPS)*, Pittsburgh, PA, July 2011.

[20] Steel, E. and G. Fowler, Facebook in privacy breach. The Wall Street Journal, October 2010.