future internet

MDPI

Article

User Perception of Facebook App Data Access: A Comparison of Methods and Privacy Concerns

Jennifer Golbeck * and Matthew Louis Mauriello

Human-Computer Interaction Lab, University of Maryland, College Park, MD 20742, USA; golbeck@cs.umd.edu
* Correspondence: jgolbeck@umd.edu; Tel.: +1-301-405-7185

Academic Editors: Salvatore Carta and Ludovico Boratto
Received: 22 February 2016; Accepted: 11 March 2016; Published: 25 March 2016

Abstract: Users share vast amounts of personal information online, but are they fully aware of what information they are sharing and with whom? In this paper, we focused on Facebook apps and set out to understand how concerned users are about privacy and how well-informed they are about what personal data apps can access. We found that initially, subjects were generally under-informed about what data apps could access from their profiles. After viewing additional information about these permissions, subjects' concern about privacy on Facebook increased. Subjects' understanding of what data apps were able to access increased, although even after receiving explicit information on the topic, many subjects still did not fully understand the extent to which apps could access their data.

Keywords: social media; privacy; usability; apps

1. Introduction

Social media users are concerned about privacy. In the study we present here, only four out of 120 subjects reported they were "Not at all" concerned about privacy on Facebook. However, despite a wide range of media reports about the consequences of oversharing and stories about how data can be used in unintended ways, people continue to interact, share data, and use apps online despite their concerns.

Are users continuing to share because they are aware of the privacy risks and have made an informed choice about what they are comfortable sharing, or are they operating under false assumptions or without the knowledge they need to make an informed choice?

In this study, we focus specifically on the personal information the Facebook apps can access on a user's profile. These apps serve as an example and case study for broader questions about user understanding of privacy in social media.

We set out to answer three research questions:

RQ1: How informed are users regarding the privacy risks of using Facebook apps?
RQ2: Will viewing additional information about what Facebook apps can access affect the way users feel about the related privacy risks?
RQ3: Are some methods of sharing this information more effective at educating users about the information that apps can access?

To answer these questions, we conducted a between-subjects experiment with 120 subjects. Subjects completed a survey indicating their concern about Facebook privacy and their beliefs about what data Facebook apps could access. Then, they were divided into conditions where they viewed either the Facebook privacy policy or the Take This Lollipop interactive horror film (Figure 1). Then, subjects re-took the survey so we could judge if their feelings and beliefs had changed.

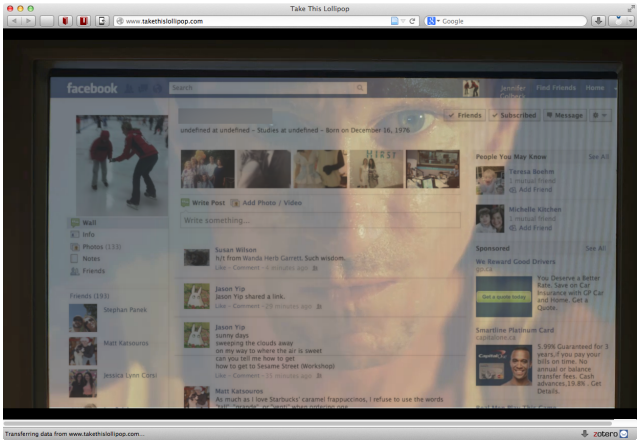

Figure 1. A screen capture of the creepy Facebook Stalker looking at a person's profile, taken as a screen capture from the Take This Lollipop video, the app used in our study.

We found substantial increases in privacy concerns and in the number of personal data attributes that our subjects believed apps could access. However, we also found that many users were still unclear about what data Facebook apps could access.

2. Related Work

Since social media started emerging as a major paradigm of internet use in the early-to-mid 2000s, there have been studies of users' concerns and privacy preferences. Studies of how people choose to share information in social media, their privacy concerns, and their awareness about these issues has been covered in [1–3] to name a few. These studies took place in 2006 and 2007, and the landscape has changed a lot since then, particularly in terms of the privacy controls available to users and in how publicly information is shared by default.

As privacy options became more sophisticated, research found that users were underutilizing these controls [4]. Tools to help users manage their privacy settings were even proposed [5].

More recent work has looked specifically at users' privacy concerns and utilization of privacy settings in these environments.

In 2009, Debatin *et al.* [6] studied users' privacy concerns in Facebook. Their subjects claimed to understand privacy issues but generally believed others were more at risk for privacy invasion than they themselves were. The authors attributed users' "lax attitude" to a number of factors, including psychological effects, the way people used the sites, and the fact that there was high gratification from use which led to downplaying the risks.

The specific privacy concerns of students on social media and its implications for education were addressed in [7]. Experimental work in this space, which compared students' perceptions of danger before and after exposure to privacy-related information found, in their experimental configuration, no significant differences. They concluded that the students, as digital natives, were already well aware of the privacy risks associated with using social media [8].

Litt [9] found differences in utilization of privacy features of social networking sites based on factors like age, gender, and experience.

In [10], the authors built a model of social network usage considering users' privacy concerns and trust. They showed that social network use was negatively correlated with privacy concern but that his could be mitigated by building trust with users. These results echo earlier work from 2009 that showed users' trust in one another and in an online communities' information sharing norms mitigated privacy concerns [11].

Ref. [12] discusses a privacy feedback tool designed to help users better understand their identity exposure online. While we do not have users interact with this tool specifically, we do have them

look at information sources that show users what data Facebook apps can collect, thereby revealing information about how exposed a user's data is to these apps.

Most closely related to our work is a 2011 study that investigated how users interacted with and understood Facebook apps' data access [13]. The study found that many users misunderstood or were confused by the policies that governed apps' access to their data. They also found that subjects' behavior or knowledge were not necessarily predictive of their level of privacy concern. Instead, privacy attitudes tended to change if the user personally experienced an adverse privacy event on Facebook. This is similar to the results from [6] discussed above; they found that personal, negative events had a big impact on users, but knowledge of bad events happening to others generally did not have much impact.

This could be because there is not a good understanding among users about what information apps access from a user's profile, and only adverse events really make the point to users. Facebook reveals some information about what data apps will have access to when users install it, and users are left to rely on this and on their own understanding of Facebook's privacy policies in this context. Generally, this information seems to be insufficient for users to fully understand the information they are sharing with an app. This motivated the work in [14], which studied a large number of apps to understand the type of access they requested to users' data. This type of profiling could be important for understanding if apps are over-requesting data access, and thus whether users need to be warned about agreeing to more expansive permissions.

3. Experimental Design

In this experiment, we wanted to understand how informed users are about Facebook app data access privileges, and to study the impact that viewing information about these privileges would have on users' privacy concerns and perceptions.

To achieve this, we administered a pre-test to gauge subjects' privacy concerns and perceptions. The answers from this initial survey are used to help us answer RQ1 described above. Then, subjects viewed information about how Facebook apps access personal data in one of four different conditions. After that, we re-administered most of the questions from the pre-test to see if and how user perception and concerns had changed.

Our exact process was as follows:

1. Obtain informed consent
2. Collect basic demographic information
3. Administer pre-test survey questions
4. Privacy information conditions—subjects were randomly assigned to one of four conditions (described below) that showed them information about what data Facebook apps can access.
5. Re-administer surveys as post-test questions to see how options may have changed after seeing the privacy information.

3.1. Pre- and Post-Test Questionnaires

Our pre-test was broken into two main sections: demographic and background questions, and Facebook-specific questions about privacy concern and the perception of what is shared. This latter group of questions was repeated in the post-test.

3.1.1. Demographic and Background Questions

We collected basic demographic information about our subjects: age, gender, the country where they grew up, and education level. We used this to determine if any demographic features impacted subjects' privacy attitudes.

Next, we wanted to gain a basic understanding of subjects' privacy attitudes. We included the Westin/Harris Privacy Segmentation Model [15,16], which uses three questions to group users into three categories: privacy fundamentalists, privacy pragmatists, and privacy unconcerned.

This survey has three statements, to which users respond "strongly disagree", "somewhat disagree", "somewhat agree", or "strongly agree":

1. Consumers have lost all control over how personal information is collected and used by companies.
2. Most businesses handle the personal information they collect about consumers in a proper and confidential way.
3. Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.

Privacy fundamentalists agree with statement 1 and disagree with statements 2 and 3. Privacy unconcerned subjects disagree with statement 1 and agree with statements 2 and 3. All other subjects are considered privacy pragmatists [15,16].

In addition, we included questions adapted from the survey instrument in [17], designed to elicit general attitudes and behavior related to privacy online. We adapted some questions to be Facebook specific. These questions are shown in Table 1 and were rated on a 5-point Likert scale from "Never" to "Always" in accordance with the initial survey design.

Table 1. Questions regarding general online privacy concerns. Each question is rated on a 5 point Likert scale from "Never" (1) to "Always" (5), except for the final question which is shown as the percentage of yes answers.

Question	Average Score
Do you...	
read a website's privacy policy before you register your information?	2.21
look for a privacy certification on a website before you register your information?	2.48
read license agreements fully before you agree to them?	1.79
block people on Facebook that you do not want to see your information?	3.63
use apps on Facebook?	59.1%

In the second half of the pre-test, we asked users about their Facebook-specific questions. These were also adapted from questions in the [17] survey instrument. Subjects answered each on a 5-point Likert scale ranging from "Not at all" to "Very much" in accordance with the original survey design. These questions are shown in Table 2. Significant increases are marked * for $p < 0.05$ and ** for $p < 0.01$.

Table 2. Answers pre- and post-test to questions about concern Facebook apps. Values are on a 5-point Likert scale ranging from "Not at all" (1) to "Very much" (5). Significant increases are marked * for $p < 0.05$ and ** for $p < 0.01$.

Concern	Pre-test Avg.	Post-test Avg.	Change	
In general, how concerned are you about your privacy while you are using Facebook?	3.533	3.925	0.392	**
Are you concerned...				
that Facebook will sell or release your personal information?	3.483	3.833	0.350	**
that you are asked to grant access to too much personal information when you install a Facebook app?	4.283	4.258	-0.025	
about online identity theft via Facebook?	2.867	3.508	0.642	**
about people you do not know obtaining personal information about you from your Facebook use?	3.683	4.058	0.375	**
that content you post on Facebook may be seen by people other than those for whom you intended it?	3.858	4.183	0.325	**
that a Facebook app could post to your timeline in your name?	4.125	4.183	0.058	
that a seemingly legitimate Facebook app may be fraudulent?	3.833	4.042	0.208	*
that Facebook apps could collect your personal data?	4.058	4.158	0.100	
that Facebook apps could sell your personal data?	4.050	4.158	0.108	

Finally, we asked subjects to tell us if they believed Facebook apps could or could not access specific types of personal information These are shown in Table 3.

Table 3. Fact-based questions about information Facebook apps can access. The percentage of "yes" responses are shown. Significant increases are marked * for $p < 0.05$ and ** for $p < 0.01$.

Question	Pre-test	Post-test	Change	
From what you know right now, when you install a Facebook app, do you think it has access to the following information?				
Your personal information (name, gender, profile photo)	98.3%	99.2%	0.8%	
Your friend list	92.5%	95.8%	3.3%	
Your profile information (education and work history, relationship status, religion, *etc.*)	88.3%	91.7%	3.3%	
Your birthday	90.8%	90.8%	0.0%	
Your likes (*i.e.*, pages you like)	85.0%	94.2%	9.2%	*
Your status updates	69.2%	85.0%	15.8%	**
Photos and videos you upload	65.8%	88.3%	22.5%	**
Comments on your content (e.g., photos or status updates)	62.5%	79.2%	16.7%	**
Your friends' profile information	66.7%	80.8%	14.2%	**
Your friends' posts that appear on your news feed	57.5%	85.8%	28.3%	**
Comments on your friends' posts (from you and others)	53.3%	72.5%	19.2%	**
Posts you made on your timeline	74.2%	91.7%	17.5%	**
Comments on your timeline posts (by others)	66.7%	85.0%	18.3%	**
Your current location	82.5%	84.2%	1.7%	
Your contact information (email, phone, address)	85.0%	83.3%	-1.7%	
Your private messages to friends	26.7%	40.0%	13.3%	**
Your chat logs	23.3%	40.0%	16.7%	**

With the right permissions, apps can access any of the data points listed here, though not all apps can do it all the time, and users have the ability to deny this access in some cases. Some information, like name, gender, and profile photo, can be accessed by all apps with basic permissions. Other information can be accessed, but only when apps explicitly request extended permissions.

There are also varying levels of extended permissions. For some extended permissions, a user has no way to deny the access except by refusing to install the app. In other cases, the user can install the app but deny access. For very sensitive types of information, like access to a user's inbox, clear additional dialogue boxes are shown to alert users about the permission they are granting.

In Table 3, items highlighted in green can be accessed by all apps. Items highlighted in yellow can be accessed through extended permissions that the user cannot opt out of; *i.e.*, if an app requests it, the user cannot install the app without granting permission. Items highlighted in pink can only be accessed through an optional opt-in extended permission request.

Thus, we might expect some users to say apps cannot access certain data points, even if they know that apps can technically get them, because the users would choose to deny access.

3.2. Conditions

Subjects viewed information about what data apps could access on Facebook. We had three diverse conditions and a fourth condition that combined the first three. Note that our goal was not to isolate and measure the impact of specific attributes of each condition, but rather to survey a range of approaches for communicating privacy information.

Condition 1: Privacy Policy—Subjects were instructed to read the Facebook Data Use Policy regarding personal information [18] and Websites and Applications [19].

Condition 2: Take This Lollipopr—"Take This Lollipop" is an interactive horror movie that integrates a viewer's Facebook profile information. A creepy stalker views the user's profile before mapping a route to their current location and drive there in a frenzy with the user's picture taped to his dashboard. The movie illustrates the wealth of profile information that an app can access (see Figure 1) in a context that connects it with risk.

Although the app requests many extended permissions when a user installs it, and these are explicitly enumerated (see Figure 2), when it launched, even users experienced with Facebook privacy settings expressed surprised at how much data it displays. For this reason, we chose it as an app that illustrates the data that can be obtained through Facebook as well as one that presents it in an engaging, entertaining, and risk-oriented context.

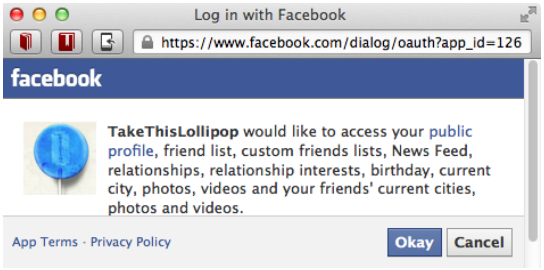

Figure 2. Data access requested by Take This Lollipop.

Condition 3: Facebook App Permissions App—In this condition, participants were asked to install an app that we developed. This provided an interface to explore their data, and it focused on what Facebook calls "basic info": Name, Profile Picture, Gender, User ID, Friends List, and any other information made public. Beyond this, we only request two other types of data: access to the user's news feed as well as an attribute that shows if the user owns any Facebook Pages or Applications. Users can deny this request.

The approach of our app differs from Take This Lollipop, which requests extensive extended permissions. The "basic" information we use is commonly accessed by all applications, so our app essentially shows what almost every app is able to access.

After a user installs the app, the most recent data from their profile is collected and then redisplayed to the user in different interactive ways using jQuery and standard HTML/CSS display widgets. The final information display is organized into five areas: basic information, a friends list, recent news items, recent page likes, and ownership permissions on pages or groups within the Facebook platform. Figure 3 shows two example tabs from this app.

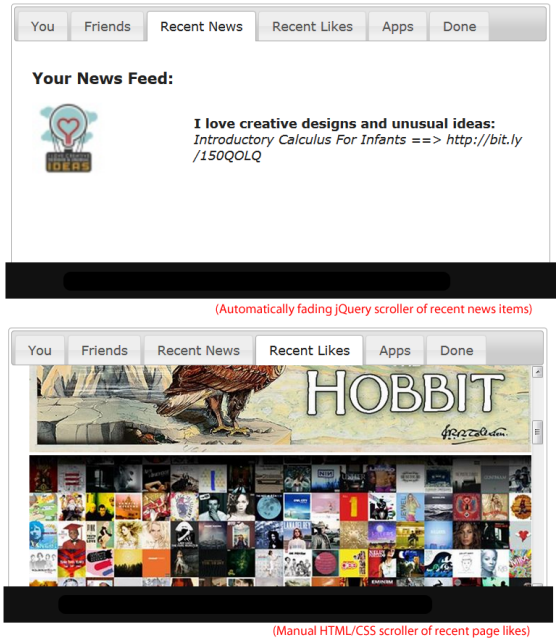

Figure 3. The interface of the Facebook Data App.

Condition 4: All of the above—Subjects in condition 4 viewed all of the information described above: the privacy policies, Take This Lollipop, and the App Permissions App.

3.3. Subjects

We solicited for subjects through mailing lists and posts to social media channels. We received complete data from 120 subjects. Gender breakdown includes 71 female, 47 male, and two unreported. Age ranged from 18- to 66-years-old with an average of 32.3 years and a median of 30. Our subjects skewed high on the educational background, with one having completed some high school, six completing some college, 37 with bachelors degrees, 58 with masters degrees, and 18 with doctorates.

This study is essentially a look at the effectiveness of different methods for conveying privacy information to users. As such, we treat it like a usability analysis. In that case, our 120 subjects gives us results close to the 99% confidence level at detecting the effectiveness of each method [20].

4. Results

For clarity in the text, significance levels will be indicated with a * for $p < 0.05$ and ** for $p < 0.01$. All tests unless described otherwise are paired t-tests comparing scores from the pre-test and post-test. Since each set of data required many comparisons, we used a Bonferroni correction where appropriate.

4.1. Overall User Understanding of Privacy Risks

The results in Table 2 show subjects' opinions about Facebook apps' access rights before and after viewing the information. On average, subjects generally believed the basic information was accessible more than the non-optional extended permission data, and both were available more than the optional extended permission data. That said, even for the basic information that all apps can access, we did not see 100% of users believing that apps could access it, even after viewing the information in the conditions that clearly indicated what was given to apps.

For the non-optional extended permission data, which any app can request access to and for which users cannot deny permission (except by refusing to install the app), we saw significant increases in the percentage of users who believed apps could access this data. However, few of these saw over 90% of users believing apps could access the data, let alone 100% of users.

Finally, for the most private data (accessible to apps, but only through extended permission requests that the user can deny), a high percentage of users believed contact information was made available to apps. Many fewer users believed chat logs and messages (both of which reside in a user's Facebook inbox) were accessible. It is possible that some users would say this information is inaccessible since they would personally deny access to apps that requested it. It is also possible that the way in which apps can get to this information is not made clear by any of the privacy information sources.

Looking at all of these data points, we see that users are under-informed about what information apps can access, and though education about the data access permissions can help, users still underestimate the amount of information that apps can access. This, in turn, has implications for how they make decisions. We discuss this further below.

We then divided subjects into two groups: those who report using Facebook apps to those who report not using them. Forty-eight subjects claimed to not use apps ("non-users"'), while 71 do use them ("app users").

Non-users were significantly* more likely than app users to believe that apps could access Status Updates, photos, a user's content and comments, newsfeed data, comments on friends' posts, timeline posts, and others' comments on timeline posts. This data is shown in Table 4. This shows that people who are using apps are generally quite under-informed about what personal information they are handing over.

Table 4. This table shows differences in the pre-test percentage of app users and non-users who believe Facebook apps can access certain types of data. Differences are significant in all cases for $p < 0.05$. We see that app users are significantly less likely to believe that apps have access to this data.

Data	Non-users	App users
Status Updates	81.3%	60.6%
Photos	77.1%	57.7%
A user's content and comments	79.2%	52.1%
Newsfeed data	72.9%	46.5%
Comments on friends' posts	79.2%	36.6 %
Timeline posts	87.5%	54.8%
Others' comments on timeline posts	83.3%	56.3%

Among app users, post-test perception about what data Facebook can access significantly increased** for nearly all items: accessing likes, photos, content and comments, friend lists, friend information, newsfeed data, private messages, chat logs, comments on friends' posts, timeline posts, and timeline comments. For non-app users, concern increased regarding apps accessing status updates**, photos**, chat longs*, and timeline posts**.

We also hypothesized that pre-existing concern about privacy might influence the results. We applied the Westin/Harris Privacy Segmentation Model described above and found our sample contained 31 Privacy Fundamentalists, 88 Privacy Pragmatists, and no Privacy Unconcerned subjects.

Not surprisingly, Fundamentalists started out with more overall concern about privacy on Facebook compared with Pragmatists (3.935 *vs.* 3.375*), concern that Facebook would sell their data (3.935 *vs.* 3.307*) and that unintended users would see their data (4.27 *vs.* 3.7*).

In the pre-test, significantly* more Fundamentalists than Pragmatists believed apps could access their content and comments, friends' information, newsfeed, private messages, and contact information. In the post-test survey, fundamentalists saw no significant changes in their concerns or beliefs about what data apps could access, while Pragmatists saw significant increases in 17 out of 27 survey questions.

It is worth noting that privacy Pragmatists and Fundamentalists are not parallel groups to app users and non-users. There was no significant difference in the percentage of app users between Fundamentalists and Pragmatists (50% *vs.* 65%, respectively).

4.2. Overall User Privacy Concern

Overall, we saw significant increases in concern about a number of factors after subjects had viewed the privacy information (across all conditions). This data is presented in Table 2 along with significance levels.

Overall concern about privacy on Facebook significantly increased 9.8% on the post-test, from an average of 3.53 to 3.93. Increases also appeared in concern about Facebook selling/releasing data, identity theft, unknown people accessing a subjects' data, unintended people viewing the data, and seeming legitimate apps being fraudulent. It is worth noting that for the concerns that did not see a significant increase, initial concern was quite high, over 4 on a 5 point scale for all factors. This left little room for increase.

4.3. The Impact of Privacy Communication Techniques

Increases in concern and perception varied based on which condition subjects interacted with between the pre- and post-tests. Table 5 shows the data for each group on the questions described above.

The "Privacy Policy", "Take This Lollipop", and "All of the above" conditions all resulted in significantly higher concerns and perceptions about what data apps on Facebook could access. Specifically, overall concern and concern about identity theft and unknown people accessing personal information increased for all three conditions.

The "Take This Lollipop", and "All of the above" conditions heightened user concern and awareness the most often. "Take This Lollipop" led to increases in five of 10 concern questions, and "All of the above" brought about increases in eight of 10; the two exceptions were items on which the initial concern ratings were very high.

Similarly, "Privacy Policy", "Take This Lollipop", and "All of the above" conditions all saw significantly higher percentages of users believing apps could access specific data. For each, seven out of 17 perceptions significantly increased.

The exception here is our App Permissions App, which resulted in no increased concern and two significant decreases in perception about what data apps can access.

To understand what users were actually learning, we first looked at what information each condition communicated to users. If a condition explicitly states that apps can access certain data points, ideally all users will understand the app can access that info. If a condition does not mention or illustrate access to a particularly data point, then any significant increases in user perception about app access may be a result of paranoia or some other effect.

In Table 5, rows have been highlighted indicating the information a condition specifically showed that apps could access that data point.

The Facebook privacy policies clearly state that all apps can access a user's Name, Profile Picture, Gender, User ID, Friends List, any other information a user has made public, and this same information for each friend. It also says that an app may access "additional information, such as stories, photos or likes" with additional permission, but it does not enumerate the data points beyond the examples.

Take This Lollipop requests a long list of permissions (see Figure 2). News Feed access includes access to comments from friends and those that a user has posted. Facebook users would know that their News Feed includes this information, and the "Take This Lollipop" video clearly shows it.

Our App Permissions App requests only a basic set of information (see Figure 4). Note that the details of "public profile" appear when the user hovers over that link in the privacy information. This notification makes it clear that we will access the user's Name, age range, profile picture, gender, language, country, friend list, and News Feed.

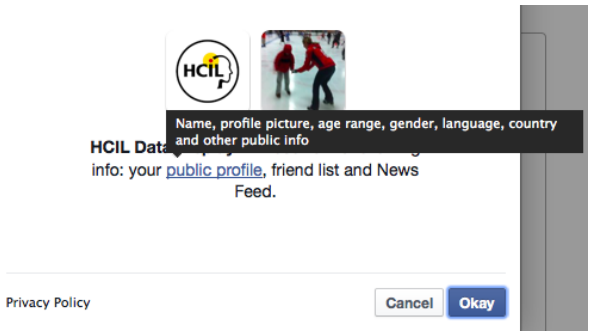

Figure 4. Data access requested by our App Permissions App.

There is a difference in the way Take This Lollipop and the App Permissions App show access to the News Feed. In Take This Lollipop, it is shown as the News Feed appears to users on the Facebook Site. In the App Permissions App, status updates from the News Feed are shown individually, but they are shown out of the context of the Facebook interface.

Table 5. Answers to survey questions pre- and post-test grouped by condition. Significant changes from pre- to post-test are shown with * for $p < 0.05$ and ** for $p < 0.01$. When a condition indicates that a particular data point can be accessed by an app, it is highlighted in yellow.

Question	Privacy Policy			Lollipop			App Permissions App			All of the above		
	Pre-Test	Post-test	Change	Pre-Test	Post-test	Change	Pre-Test	Post-test	Change	Pre-Test	Post-test	Change
In general, how concerned are you about your privacy while you are using FB?												
Are you concerned...												
In general, how concerned are you about your privacy while you are using FB?	3.417	3.778	0.361 **	3.471	3.971	0.500 **	3.462	3.577	0.115	3.875	4.458	0.583 **
that FB will sell or release your personal information?	3.556	3.750	0.194	3.412	3.971	0.559 **	3.385	3.615	0.231	3.583	4.000	0.417 *
that you are asked to grant access to too much personal information when you install a FB app?	4.250	4.083	-0.167	4.382	4.500	0.118	4.231	3.923	-0.308	4.250	4.542	0.292
about online identity theft via FB?	2.583	3.167	0.583 **	2.882	3.676	0.794 **	3.077	3.231	0.154	3.042	4.083	1.042 **
about people you do not know obtaining personal information about you from your FB use?	3.417	3.750	0.333 **	3.706	4.206	0.500 **	3.846	3.808	-0.038	3.875	4.583	0.708 **
that content you post on FB may be seen by people other than those for whom you intended it?	3.944	4.000	0.056	3.588	4.147	0.559 **	3.846	4.000	0.154	4.125	4.708	0.583 **
that a FB app could post to your timeline in your name?	4.222	4.333	0.111	4.029	4.118	0.088	3.962	3.846	-0.115	4.292	4.417	0.125
that a seemingly legitimate FB app may be fraudulent?	3.889	4.000	0.111	3.882	4.176	0.294	3.769	3.731	-0.038	3.750	4.250	0.500 **
that FB apps could collect your personal data?	4.028	4.056	0.028	4.000	4.088	0.088	4.154	4.000	-0.154	4.083	4.583	0.500 **
that FB apps could sell your personal data?	4.056	4.111	0.056	4.000	4.147	0.147	4.038	3.885	-0.154	4.125	4.542	0.417 **
From what you know right now, when you install a FB app, do you think it has access to the following information?	(values given in percentages)											
Your personal information	100.0	100.0	0.0	94.1	97.1	2.9	100.0	100.0	0.0	100.0	100.0	0.0
Your profile information	88.9	94.4	5.6	85.3	94.1	8.8	96.2	80.8	-15.4 *	83.3	95.8	12.5
Your status updates	69.4	88.9	19.4 **	73.5	88.2	14.7	76.9	73.1	-3.8	54.2	87.5	33.3 **
Comments on your content	69.4	83.3	13.9 **	61.8	88.2	26.5	61.5	61.5	0.0	54.2	79.2	25.0
Your friend list	91.7	91.7	0.0	88.2	94.1	5.9	96.2	100.0	3.8	95.8	100.0	4.2
Friends' posts that appear on your news feed	69.4	86.1	16.7	41.2	85.3	44.1 **	69.2	80.8	11.5	50.0	91.7	41.7 **
Comments on your friends' posts	63.9	80.6	16.7	47.1	76.5	29.4 **	53.8	57.7	3.8	45.8	70.8	25.0 *
Posts you made on your timeline	80.6	94.4	13.9 *	70.6	88.2	17.6	80.8	84.6	3.8	62.5	100.0	37.5 **
Comments on your timeline posts	75.0	94.4	19.4 **	64.7	88.2	23.5 **	69.2	61.5	-7.7	54.2	91.7	37.5 **
Your likes	83.3	97.2	13.9 *	79.4	94.1	14.7	92.3	92.3	0.0	87.5	91.7	4.2
Photos and videos you upload	77.8	91.7	13.9	58.8	88.2	29.4 **	69.2	73.1	3.8	54.2	100.0	45.8 **
Your birthday	91.7	97.2	5.6	85.3	91.2	5.9	96.2	76.9	-19.2	91.7	95.8	4.2
Your friends' profile information	75.0	80.6	5.6 *	61.8	79.4	17.6	73.1	73.1	0.0	54.2	91.7	37.5 **
Your private messages to friends	36.1	50.0	13.9	17.6	44.1	26.5 **	26.9	23.1	-3.8	25.0	37.5	12.5
Your chat logs	33.3	50.0	16.7 **	14.7	50.0	35.3 *	23.1	19.2	-3.8	20.8	33.3	12.5
Your contact information	83.3	83.3	0.0	85.3	85.3	0.0	92.3	69.2	-23.1 *	79.2	95.8	16.7
Your current location	83.3	86.1	2.8	76.5	79.4	2.9	84.6	73.1	-11.5	87.5	100.0	12.5

Seventeen out of 20 significant increases in user perception about what data apps can access occurred when a condition showed that the data could be accessed. At the same time, both the privacy policy condition and Take This Lollipop had large significant increases in the percentage of users who believed apps could access their chat logs, even though neither condition showed that such data was available. There was also a large significant increase in the percentage of subjects who believed apps could access private messages to friends after watching Take This Lollipop; again, the video does not show that such access is possible.

The App Permissions App had two significant decreases in the percentage of users who thought apps could access the user's profile information and contact information. The app did not show that it could access contact information. It did show access to a user's profile information (education work history, relationship status, religion, *etc.*), but only if the information had privacy settings that made it publicly visible. For users with privacy restrictions, this information may not have appeared thus leading users to conclude apps could not access it.

5. Discussion

A number of insights arise from the results of this study.

First, we found that users are concerned about privacy on Facebook, particularly with respect to the information apps can access. At the same time, users were generally under-informed about what information Facebook apps can access. There were no cases where 100% of users believed apps could access the information we asked about, and in many cases, a large percentage of users were unaware that apps could access certain data. Even more dramatically, our subjects who reported using apps on Facebook were significantly less likely to know what data the apps could obtain. In many cases, fewer than 60% of app users were aware that apps could access particular data points.

We found that education can improve user understanding of what apps can access. In parallel, this education also increased users' concerns about the accompanying privacy risks. The more information people saw, the more concerned they became. Subjects who looked at information from all three information sources had the highest post-test levels of concern.

At the same time there were some "unjustified" increases in user perception. For three data points, we saw large increases in the percentage of users who believed apps could access them, even though the information subjects looked at between the pre- and post-test did not indicate that apps could in fact get to this data. While these users were not incorrect in thinking apps could see those data points, we have no clear explanation for why their opinions changed between the tests. Similarly, we saw significant decreases in the percentage of users who thought apps could access two types of data after they viewed the App Permission App.

These issues lead to important areas of future work.

Each of the information sources that we used had different attributes both in terms of the information they presented, the detail that was used, and the style of presentation. We did not examine this issue specifically, but extrapolating from these results, it appears that the more dramatic style of Take This Lollipop did not lead to greater understanding of what apps could access; we saw more significant increases with the privacy policy condition. However, there were more increases in *concern* about privacy with Take This Lollipop. In addition, we saw some significant increases in user belief that apps could access certain data points, even when the information sources did not show that these could be accessed.

We hypothesize that this could be because the personalized and horror-oriented nature of the Take This Lollipop video mimics some of the effects of a personal negative privacy event. As discussed in [6] and [13], when a user personally experiences a negative consequence related to privacy, it is more effective at increasing users' privacy awareness and concern.

At the same time, the App Permissions App, which showed samples of what data an app could access, was less effective at increasing user understanding of data access policies. Subjects in this condition also had no significant increases in privacy concern. It is unclear why users' perception of

what data apps could access decreased in some cases, but understanding this is an important question to follow up on. If certain aspects of an interface can mislead users into falsely believing their data is private, those should be isolated and included as important attributes to avoid in design guidelines going forward.

A controlled study that looks at information provided to users, the presentation style, and the effect it has on both concern and perception will likely yield important insights about how to best inform users about the information they are sharing. It will also help researchers and designers understand what might cause the most concern in users, which should be balanced with the risks of the behavior.

Who exactly will provide this information to users is another important issue to consider. There is a question about whether social media sites like Facebook have an incentive to let users know exactly what apps can access and how. We found an increase in privacy concerns after users became more informed about data access policies. This could lead users to interact less with apps, thus decreasing engagement with a site and, in turn, reducing its profits. If an under-informed user base is more profitable, it may fall to third parties to fully educate users about what they are sharing and what the risks are when they make the choice to install.

Finally, we see this study as one step in a greater research agenda of integrating Human-Computer Interaction (HCI) and cybersecurity. Privacy and security research has often overlooked the human element. Usability of security features can be low, leading to riskier behavior from users. Poor presentation of privacy information can lead to uninformed users making bad choices about what personal information to share and what apps to interact with. Better understanding users and their behavior in context can lead to improved security and privacy.

6. Conclusions

In this study, we looked at users' concerns and perceptions about privacy, particularly in the context of Facebook apps. We conducted an experiment where subjects were surveyed about their concerns and perceptions regarding what data Facebook apps could access. They completed a survey, then viewed information about Facebook app data access, and re-took the survey.

While subjects did report concern about privacy, we found they do not have a full understanding of how that information is shared with apps. Subjects who reported using Facebook apps were significantly less informed about what data those apps could access when compared with subjects who did not use them.

We compared the effectiveness of three methods for educating users about app data access in four conditions. We found that, overall, viewing this material increased privacy concern and understanding about what information apps could access. At the same time, some methods were more effective than others. Future work is needed to understand the dynamics of communication mechanisms, design, attention, style, and other factors that affect understanding and concern.

Finally, this study is a first step in a larger space of work connecting humans, HCI, and cybersecurity. People ultimately choose what data to share and how to protect it. They cannot do this in the optimal way without a full understanding of how it is shared, with whom, and what could result from that sharing. There are important research questions in this area for psychology, cognitive science, communications, computer science, and design. We hope this work is a step in the direction of better understanding initial questions in this expanding space of research.

Acknowledgments: This material is based upon work supported, in part, by the Maryland Procurement Office under contract H98230-14-C-0127. Any opinions, findings and conclusions or recommendations express in this material are those of the author(s) and do not necessarily reflect the views of the Maryland Procurement Office

Author Contributions: J.G. conceived and designed the experiments; M.L.M. designed the app; J.G. and M.L.M. performed the experiments; J.G. analyzed the data; J.G. and M.L.M. wrote the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Acquisti, A.; Gross, R. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Privacy Enhancing Technologies*; Springer: Berlin, Germany; Heidelberg, Germany, 2006; pp. 36–58.
2. Dwyer, C.; Hiltz, S.R.; Passerini, K. Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace. In Proceedings of the AMCIS, Keystone, CO, USA, 9–12 August 2007; p. 339.
3. Strater, K.; Richter, H. Examining privacy and disclosure in a social networking community. In Proceedings of the 3rd Symposium on Usable Privacy and Security, Pittsburgh, PA, USA, 18–20 July 2007; pp. 157–158.
4. Strater, K.; Lipford, H.R. Strategies and struggles with privacy in an online social networking community. In Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 1, Liverpool, UK, 1–5 September 2008.
5. Fang, L.; Kim, H.; LeFevre, K.; Tami, A. A privacy recommendation wizard for users of social networking sites. In Proceedings of the 17th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 4–8 October 2010.
6. Debatin, B.; Lovejoy, J.P.; Horn, A.K.; Hughes, B.N. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *J. Comput.-Mediat. Commun.* **2009**, *15*, 83–108.
7. Vidal, C.E.; Martínez, J.G.; Fortuño, M.L.; Cervera, M.G. Actitudes y expectativas del uso educativo de las redes sociales en los alumnos universitarios. *RUSC* **2011**, *8*, 171–185.
8. Gutiérrez, F.J.H.; Bejarano, H.J.R. La asunción de los peligros relacionados con la privacidad en Internet y en redes sociales por parte de los universitarios españoles. *index.comunicación* **2015**, *5*, 107–121.
9. Litt, E. Understanding social network site users' privacy tool use. *Comput. Hum. Behav.* **2013**, *29*, 1649–1656.
10. Lin, S.W.; Liu, Y.C. The effects of motivations, trust, and privacy concern in social networking. *Serv. Bus.* **2012**, *6*, 411–424.
11. Nov, O.; Wattal, S. Social computing privacy concerns: antecedents and effects. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Boston, MA, USA, 4–9 April 2009.
12. Emanuel, L.; Bevan, C.; Hodges, D. What does your profile really say about you? Privacy warning systems and self-disclosure in online social network spaces. In *CHI '13 Extended Abstracts on Human Factors in Computing Systems*; ACM: New York, NY, USA, 2013; pp. 799–804.
13. King, J.; Lampinen, A.; Smolen, A. Privacy: is there an app for that? In Proceedings of the Seventh Symposium on Usable Privacy and Security, Pittsburgh, PA, USA, 20–22 July 2011.
14. Wang, N. Third-party applications' data practices on facebook. In *CHI '12 Extended Abstracts on Human Factors in Computing Systems*; ACM: New York, NY, USA, 2012; pp. 1399–1404.
15. Interactive, H. Privacy On and Off the internet: What Consumers Want. In *Harris Interactive, Conducted for Privacy and American Business*; Technical report for Harris Interactive: New York, NY, USA, 2 February 2002.
16. Kumaraguru, P.; Cranor, L.F. *Privacy Indexes: A Survey of Westin's Studies*; Institute for Software Research International, School of Computer Science Carnegie Mellon University: Pittsburgh, PA, USA, 2005.
17. Buchanan, T.; Paine, C.; Joinson, A.N.; Reips, U.D. Development of measures of online privacy concern and protection for use on the Internet. *J. Am. Soc. Inf. Sci. Technol.* **2007**, *58*, 157–165.
18. Facebook Use Data Policy. Available online: https://www.facebook.com/about/privacy/your-info (accessed on 1 September 2014).
19. Facebook Data Use Policy. Available online: https://www.facebook.com/about/privacy/your-info-on-other (accessed on 1 September 2014).
20. Virzi, R.A. Refining the test phase of usability evaluation: How many subjects is enough? *Hum. Factors* **1992**, *34*, 457–468.