Privacy: Is There An App for That?

Jennifer King[1], Airi Lampinen[1,2,3], Alex Smolen[1]

[1] School of Information
University of California - Berkeley
102 South Hall
Berkeley CA 94720-4600, USA
{jenking,alsmola}@ischool.berkeley.edu

[2] Helsinki Institute for Information Technology HIIT / Aalto University
P.O.Box 19215
Aalto, Finland
airi.lampinen@hiit.fi

[3] University of Helsinki
Department of Social Research
P.O. Box 54
00014 University of Helsinki, Finland

ABSTRACT
Users of social networking sites (SNSs) increasingly must learn to negotiate privacy online with multiple service providers. Facebook's third-party applications (apps) add an additional layer of complexity and confusion for users seeking to understand and manage their privacy. We conducted a novel exploratory survey (conducted on Facebook as a Platform app) to measure how Facebook app users interact with apps, what they understand about how apps access and exchange their profile information, and how these factors relate to their privacy concerns. In our analysis, we paid special attention to our most knowledgeable respondents: given their expertise, would they differ in behaviors or attitudes from less knowledgeable respondents? We found that misunderstandings and confusion abound about how apps function and how they manage profile data. Against our expectations, knowledge or behavior weren't consistent predictors of privacy concerns with third-party apps or on SNSs in general. Instead, whether or not the respondent experienced an adverse privacy event on a social networking site was a reliable predictor of privacy attitudes.

Categories and Subject Descriptors
H5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

General Terms
Human Factors

Keywords
Privacy, social networking applications, Facebook, adverse privacy events

1. INTRODUCTION
Imagine—you check your Facebook page, and find your News Feed is peppered with requests from your friends: "Be my construction buddy on FarmVille!" "Help me reach the next level on Mafia Wars!" If you were tempted to spend some time raising virtual crops or robbing virtual banks with your friends, you wouldn't be alone: in June 2011, Facebook reported that over 20 million applications—the social games, utilities, and other "apps" that users enjoy— are installed every day.[1]

As social networking sites (SNSs) continue to grow in popularity and become a cumulative archive of personal information, they are ripe targets for marketers, government agencies, and online predators [2]. When it comes to privacy, Facebook has been under heavy fire in the popular press and academic writings for several years (for an overview of Facebook's history with privacy, see boyd & Hargittai [6]). The debate has mostly revolved around Facebook's privacy policies and the privacy controls the service provides to its users. Privacy issues related specifically to apps have attracted less attention, although in 2010 *The Wall Street Journal* revealed that several of the most popular apps had been transmitting identifying information to advertising and internet tracking companies [16]. While such practices explicitly violate Facebook's Terms of Service, at the same time they highlight both the complexities and vulnerabilities posed by apps.

Facebook defines its platform as "*an extension of Facebook, whose mission is to give people the power to share and make the world more open and connected.*"[2] More accurately, Platform provides a protocol (API) for third-party developers to deploy applications within the Facebook site, though the code and associated data are run from the developers' sites. In contrast, traditional gaming sites such as Yahoo!Games maintain both the game app and associated user data on its own site. On Platform users access an app and interact with it while on Facebook.com, but the code and associated user data are held at the app creator's site. The application essentially "borrows" the user data from Facebook for the purpose of providing the app.

Due to the way apps are integrated into Facebook's ecosystem, it is uncertain whether users understand that they are sharing their profile information with a party external to Facebook. Given the novelty of app platforms, we question not only whether Facebook users grasp the subtlety of the distinction between Facebook and the apps running on its platform, but also whether users understand the information-sharing model that exists beneath the veneer of raising crops or shooting bad guys.

In this paper, we set out to explore the assumption that understanding the information disclosure practices to third-party apps leads to concern about privacy and, consequently, more privacy protective behaviors. We explore what exactly Facebook users who use apps understand about them, and whether more knowledge about how apps exchange profile information is related to more privacy-conscious attitudes and behaviors. Would more privacy-concerned respondents demonstrate any differences in their knowledge or behavior? In our analysis, we pay special

[1] http://www.facebook.com/press/info.php?statistics read on June 6, 2011.

[2] http://developers.facebook.com/policy/ read on June 3, 2011

Symposium On Usable Privacy and Security (SOUPS) 2011, July 20-22, 2011, Pittsburgh, PA, USA.

attention to the respondents who are most knowledgeable about how apps function in order to better understand if knowledge is related to privacy-conscious attitudes and behaviors.

To explore these issues, we created our own app and deployed it on Platform in order to conduct a non-random, exploratory survey (N=516) on how Facebook users perceive apps, what they know about them and the platform, and how these relate to their privacy concerns. At the time the survey was conducted (March-May 2010), Facebook users had a good excuse not to know what apps were: Facebook itself did not provide a definition of them anywhere on their site. Since then, the company has added a definition that can now be found (albeit with difficulty) on their help pages.[3]

We begin with a review of our descriptive statistics about app usage, comprehension, and privacy attitudes. Next, we explore the relationship between respondents' knowledge and behavior (e.g., usage) of third-party apps and their privacy attitudes in three areas: privacy-risky practices by third party apps, privacy concerns related to other users on Facebook, and privacy concerns related to the company itself. We briefly review bivariate comparisons we made of the survey questions in order to examine key relationships. We then discuss the regression analysis we used to examine the independent effects of several groups of variables. We do not take a theoretical stance towards causality between the constructs, nor would the data we have allow us to make any causal claims. Instead, given the limited extant research into users' experiences with applications, we aim at providing a baseline for future work by means of an exploratory analysis of Facebook users' knowledge, usage, and privacy concerns about apps.

We consider privacy here as informational, based on the perception of control users have over information (data) about themselves, per the work of Alan Westin [20]. In the realm of SNSs, personal information includes the data posted by an individual (and occasionally by others) to one's online profile; the photos, comments, photo tags, and other social data users post on the site; but not the site usage data generated and collected by the service.

Theoretically, threats to privacy can be divided to two conceptual categories: social and organizational threats [13]. Social threats (or as we refer to them, interpersonal) are those related to other individuals on a social networking site, such as revealing to one's employer information intended only for one's friends. Organizational threats (or as we refer to them, institutional), on the other hand, are posed by the SNS itself or by its partners. Here, potential sources of organizational threats to privacy are both Facebook as a company as well as the companies and individuals in charge of apps on Facebook's platform. Organizational threats can include, for instance, the improper disclosure or sale of profile data. Our study looks into privacy concerns corresponding to both types of threats.

When it comes to interpersonal threats, one's personal data can be managed through Facebook's privacy settings, assuming users know of their existence and understand how they work as well as how they control who can access their profile information. However, there is also the further issue that privacy settings do not account for the problem of sharing of personal data with organizational entities. On Facebook, users have little control over this type of sharing; with respect to Platform, users can only choose to use Platform or not. At the time we conducted our study, if users installed any apps, the apps had access to all of the user's public data and a core set of non-public data without exception. The only aspect users could change is how much data applications that their friends added to their profiles have access to on the user's own profile: buried deep in one's account settings options is a screen that allows users to control what friends' apps can see via the friends' friends lists.

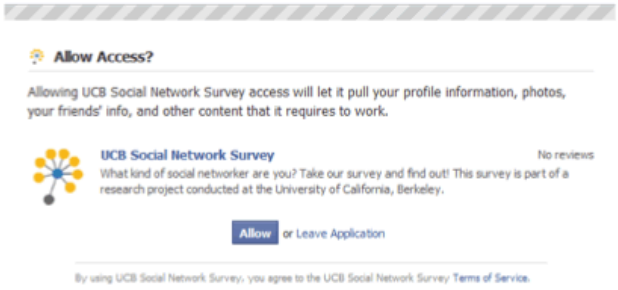


Figure 1: The Allow Access Notice (March 2010)

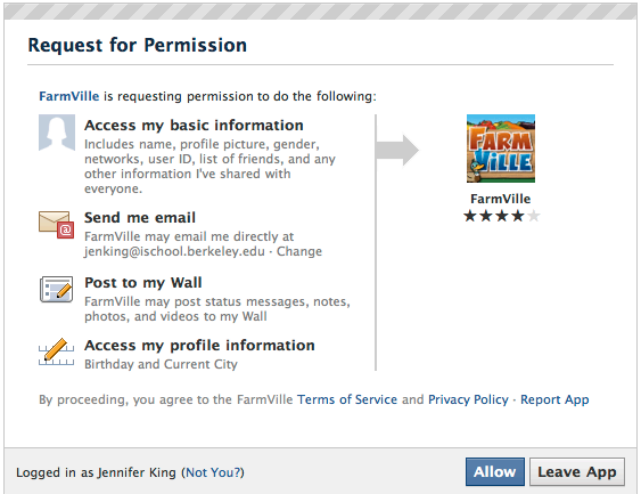


Figure 2: The New Request for Permission Notice (June 2011)

In May 2010, Facebook changed third-party application privacy settings so that only basic information is exposed to apps by default. Users are now shown the data apps request beyond the basic set via the "Request for Permission" notice that appears when users attempt to add apps. Granular permissions were also added for optional permissions (e.g. turning off wall posts by

[3] "*Applications on Facebook are designed to enhance your experience on the site with engaging games and useful features like Events and Photos. Some applications are built by Facebook developers, but most applications are built by outside developers who use Facebook's APIs and abide by Facebook's Developer Principle and Policies. Applications on Facebook allow you to play social games with your friends, remember friends' birthdays, share your taste in movies, send gifts to friends, and much more.*" http://www.facebook.com/help/new/?page=1095 read on June 3, 2011.

apps).[4] While these changes directly affect two of our survey questions that asked about the wording of the notice and about the specific profile data fields apps can access, they do not undermine the substance of our analysis. While these changes are positive and may provide users with more visibility into what data apps are requesting, we believe that the broader question of whether users who have greater knowledge of third-party application information disclosure practices behave differently is still relevant.

We claim that the core of the privacy issue concerning apps lies deeper than in poor communication or inadequate privacy controls. The information sharing model of apps is complex, still novel for many users, and does not fit with traditional understandings of how websites function. The way in which apps are embedded within Facebook makes it challenging, even visually, to draw the line between Facebook and apps that are run on its platform by third parties. The lack of visual and functional differentiation between the service and apps may nurture unwarranted expectations that some kind of a due diligence has been done when, indeed, there has often been none.

While our study focuses on Facebook and its users' relations to the apps on its platform, the use of applications is a growing phenomenon that is not limited to Facebook. Other SNSs, such as MySpace, as well as mobile platforms, such as those run by Android, Windows, and Apple, are putting apps in reach of millions of new users, marking an ongoing development towards both more deeply connected and more complex online service infrastructures. These complex connections and the way they are (not) communicated can make it hard to understand and manage how personal information is shared and stored online.

In public discussions, Facebook is repeatedly blamed for aggressively changing its privacy policies as well as the inadequate ways in which users are informed about how their information is shared. Similarly, SNS research that aims at designing for privacy is often focused on how users could be better informed and made to comprehend how the services they use function as well as the ramifications of their information sharing. Privacy, then, is framed as an informational problem: there seems to be an underlying assumption that if only users knew what was going on, they, too, would be very concerned, and hence changing their practices to be more protective of privacy. Our study indicates that reframing privacy challenges may be necessary. Platforms that describe privacy practices as objective statements may not effectively inform users about privacy risks. We conclude that better outcomes might result if platforms demonstrated in more personal and concrete ways how privacy settings impact a users' sensitive information, both in the interpersonal and institutional settings.

2. RELATED LITERATURE

In this section, we will review the existing empirical privacy research focusing on Facebook. There have been several examinations of the relationship between privacy concerns, behaviors, and knowledge. Researchers have reached a variety of conclusions, some contradictory, that are ripe for further analysis. Additionally, there has been little research examining third-party apps and the privacy challenges they pose.

[4] https://www.facebook.com/press/releases.php?p=164155

Acquisti and Gross [1] surveyed Facebook users and compared stated attitudes towards privacy with actual privacy behavior around personal information exposure. They found that even users who self-reported strong privacy concerns revealed significant amounts of personal information. It is noteworthy that this survey took place in 2006, when Facebook catered almost exclusively to college and high school students. A survey conducted by Tufekci [19] also found disjunctions between "*stated privacy concerns*" and "*actual revelation behavior*", and saw "*little to no relationship between online privacy concerns and information disclosure on online social network sites.*" Christofides et al. [8] attempted to determine how attitudes and behaviors relating to information control were associated, and what psychological factors affected these variables. They found that concern for control and disclosure were not correlated, as did Barnes [2].

Taking a different approach, Krasnova et al. [13] divided privacy concerns for users of SNSs into organizational threats and social threats. The former were concerns about information collected and used by the SNS and third parties. The latter, in contrast, were related to how others in the SNS might react to the disclosed data, such as bullying or stalking. The authors found that users revealed less information in response to organizational privacy threats, and were more conscious about what they disclosed in reaction to social privacy threats. This study suggested that concerns and behaviors do correlate, and it hypothesized that these disagreements could have resulted in part from differences between how measurements were taken when assessing concerns and behaviors. One possible interpretation is that interpersonal concerns dominate disclosure behavior, as Raynes-Goldie's [18] showed in an ethnographic study of Facebook users in their twenties who were more concerned with leakage of information across social barriers (for example, a teetotaler friend seeing their drunken photo), sometimes leading to their use of aliased profiles and regular "Wall clearings". Other findings demonstrate users' low institutional concerns of SNSs, such as Conti and Sobiesk [9] who show that the majority of users feel comfortable with the level of institutional privacy afforded by search engines, even though most did not fully trust these services or understand how to perform anonymous searches.

In addition to being connected to behavior, privacy concerns may also be affected by knowledge of privacy issues. In a study of pharmacy students, Cain et al. [7] observed an increased desire to change Facebook privacy settings after the students were given a presentation on online professionalism and how that related to their personal information shared on Facebook. Stutzman et al. [18] found that increased consumption, or comprehension, of privacy policies in SNSs—Facebook in particular—was a controlling factor in the privacy attitudes of users. The more users were aware of Facebook's privacy policies, the more concerned they were with privacy.

While privacy on Facebook has been studied extensively, research on Facebook apps and user privacy remains relatively scarce. Krasnova et al. [13] found that when viewed through the lens of organizational threats, "*users neither subjectively differentiate between who collects and uses the information they provide (OSN Provider vs. Third Parties)*". This suggests that users have more difficulty unpacking app privacy concerns.

To our knowledge, Besmer et al. [3,4,5] have the most comprehensive set of research on app privacy, and argue against the all-or-nothing permission model by presenting a prototype interface that allows a user to configure a user-application policy

[4]. The interface includes a social feedback measure of how many other users have shared a particular piece of information with an app. The authors then conducted a study of potential users of the interface with a general survey, including a Westin-style questionnaire that asked the users to use the interface with a fake set of apps that in some cases asked for excessive information. There were two evenly split categories of users: motivated and unmotivated. The motivated group generally set custom policies, while the unmotivated group accepted apps blindly.

More recently [5], the authors conducted a larger study to show that these social cues only have an effect on behavior when they are sufficiently visible. Additional research on the topic [3] examined motivations for adding apps. Most respondents reported adding apps they found through friends, as opposed to through the app directory. Very few respondents reported any privacy concerns with apps, and most demonstrated very little understanding of data collection practices of apps on Facebook, even though they had been presented with a warning screen that indicated the apps' permissions. This suggests that for some users, social factors rather than concerns about a company's privacy practices may be the primary factor that influences disclosure behavior.

3. DATA COLLECTION

3.1 Facebook Platform Survey

In order to assess the relationship between respondents' privacy attitudes and their knowledge of and behavior with third-party apps on Facebook, we applied a novel approach: we constructed a sixty-question survey and delivered it as a Facebook app. We thought this format would provide the best means to ask highly contextual questions about adding and using apps that otherwise might rely too much on respondents' memories while affording us a larger and more diverse subject pool than if we conducted individual interviews. We folded our questions about applications into a larger set of questions exploring information privacy attitudes, behaviors, and knowledge about Facebook as well as social networking sites more generally.

The survey was live on Facebook Platform from March to June of 2010. It was initially seeded through the friends lists of two of the co-creators; respondents who were on either list were flagged in the sample. The survey was also advertised on several email lists, on the Craigslist "volunteers" section in over fifteen major U.S. cities, and in a small number of ads placed on the Facebook network. Our university's name and seal were featured prominently on every page of the survey and on the app's home page on Facebook. A consent statement appeared on the first page of the survey.

In order to encourage completions (no compensation was offered), respondents were enticed to find out "*what type of Facebook user*" they were, which we calculated based on an analysis of the quantity of data in their profiles (which our app accessed via the Platform API). We classified subjects as one of four types of users: Exhibitionist, Cautious Extrovert, Intimate Sharer, and Lurker, and presented the "results" on the final page of the survey. The classifications represented four axes across two measures: the amount of information the respondent shared and their level of activity on Facebook. These classifications were for entertainment value only and were based on calculations made via the API, not the respondents' answers (this fact was disclosed on the survey completion page).

To promote recruitment, we utilized Facebook's app promotion tools, giving respondents the opportunity to publicize their "results" to their News Feed in order to encourage others to take the survey. While we were not able to track the source of our respondents, usage statistics suggest that the majority of respondents found our survey virally through their News Feed. Through this process we were able to obtain 516 usable surveys from a pool of 542 completed (we excluded any surveys where respondents indicated they were under the age of eighteen, as well as surveys with missing data). This includes 111 respondents (22% of the sample) who were on the authors' friends lists. Calculated from a total 816 survey views (this includes people who viewed the first page of the survey and chose not to complete it), our response rate was 63% percent. We randomly split respondents into two groups to evaluate the internal reliability of the questions; no significant differences were found between the groups. Respondents' Facebook user IDs were hashed for anonymization purposes, and no personally identifiable data was collected. Our design was reviewed and approved by our university's IRB.

In addition to the survey responses, we collected data about each respondent's profile (but no actual profile data) in order to compute measures of how much information people were sharing on Facebook. For most fields we computed a simple binary score (1 if the field contained data, 0 if blank) or a count if available (such as the total number of status updates and the number of status updates in the past 30 days). While detailed inferences about information sharing habits cannot be made from these counts, they provided a useful metric in addition to respondents' self-reported answers. Because privacy settings were not accessible through the API, we were not able to incorporate any information about how respondents set them compared to their own self-reported opinions about privacy issues.

3.2 Survey Design Limitations

As this is a novel method for collecting survey data, we must be clear regarding what this data can and cannot represent. First, this design has threats to both internal and external validity. We likely have response bias, specifically in the form of people who are typically not app or Platform users. Our pool generally (but not completely) lacks these users.[5] Because our primary goal was to understand what app users understood about apps, we did not feel that the general exclusion of non-Platform users would compromise our findings.

Our response pool is a convenience sample of Facebook Platform users and is not representative of Facebook's membership. Unfortunately, because only Facebook has the definitive statistics about their user population, we can only compare our sample to the limited information the company provides about their members. As a convenience sample, it raises questions as to the survey's external validity. Because of these limitations, we are

[5] Some respondents informed the authors via comments on the application's home page on Facebook that they were not typically application or Platform users and only added our application for the express purpose of completing the survey, after which they removed it.

conservative in suggesting the broader impact of this sample, but believe it can provide a useful starting point for further, more rigorous and in-depth analyses, ideally using random sampling. We do attempt to control for any influence the presence of respondents on the authors' friends list may have had in our regression analysis results.

Despite these validity threats, this survey does have two advantages over academic Facebook surveys: a larger sample size and a more diverse respondent pool. We should note that the great majority of the previous quantitative research on Facebook users has been limited to college age students. The 294 subjects in Acquisti and Gross' [1] 2006 study were 64 percent undergraduates and 25 percent graduate students; the surveys analyzed by boyd and Hargittai [6] (both in their 2009 full sample and 2010 follow-up group) were 98-99 percent submitted by students of ages 18 and 19. Though they did not specify age ranges, other studies [8,10,13,18] had survey participants that were 87 percent or greater college-age undergraduates.

Table 1: Respondent Demographics		
Gender	Male	36%
	Female	64%
Age	Mean (Range: 18-72)	35.3(9.44)
	18-24	8%
	25-34	45%
	35-44	35%
	45-54	8%
	55-64	4%
	65+	1%
Political Affiliation	Democrat	56%
	Republican	3%
	Independent	18%
	No Preference	9%
	Other	4%
	Not in US	4%
	Decline to state	7%
Race	White	78%
	African American	1%
	Asian/Pacific Islander	9%
	American Indian/Alaskan	1%
	Mixed Race	5%
	Other	2%
	Decline to state	4%
Education	<High School	0%
	HS grad	1%
	Technical/trade school	2%
	Some college, no degree	11%
	2 year college degree	3%
	4 year college degrees	27%
	Grad/professional school	54%
	Decline to state	2%
Relationship Status	Single	31%
	Married	47%
	Living w/partner	14%
	Divorced	3%
	Separated	2%
	Widowed	1%
	Decline to state	4%
Living in the U.S.?	Yes	95%
	No	5%

3.3 Respondent Demographics

Table 1 summarizes our self-reported respondent demographics. Facebook doesn't publish user demographics, but they do tell us that the average user has 130 friends, is connected to 80 pages, groups and events, and creates 90 pieces of content per month[6]. We were able to gather similar statistics from respondents' profiles using the Platform API. Our respondents' number of friends ranges from zero to 2,668, with a mean of 253 (sd=218). (Seven respondents had over 1000 friends, and 46 had over 500). Limiting the range to the 75th percentile to exclude large outliers (n=337), the mean drops to 164 (sd=84). Our respondents connected to an average of 130 (sd=172) pages, groups, and events. In the past thirty days prior to taking our survey they posted a mean of ten status updates (sd=14), five links (sd=12), ten photos (sd=27), and were tagged in an average of three (sd=7) photos.

We also divided up our respondents into two groups: the "most knowledgeable," representing 13 percent of our respondent pool,[7] and everyone else (the "less knowledgeable" 87 percent). Given that we allowed respondents to indicate "not sure" as an answer choice throughout the survey, we were not able to create a reliable subset of the "least knowledgeable" respondents in the same fashion.

Our most knowledgeable respondents were predominantly male (60 percent vs. 32 percent of the less knowledgeable), slightly (but not significantly) younger (an average of 34 vs. 36 years old), more educated (93 percent with a college education or greater vs. 81 percent), more likely to be on an author's friends list (38 percent vs. 19 percent) and more White (88 percent vs. 77 percent, but again not significantly). There were virtually no differences between the groups with regards to political affiliation, relationship status, or whether they were living in the U.S.

4. DESCRIPTIVE SURVEY FINDINGS

In this section, we review descriptive findings on respondents' use of Facebook and apps as well as their understanding and privacy concerns in relation to these two. A complete listing of the survey questions and responses is in Appendix 6. While most respondents were familiar with Facebook, apps, and how they function, the number of participants who were unsure about their knowledge is high.

4.1 Use of Facebook and Third-Party Applications

As stated above, all of the respondents were Facebook users. The vast majority of our respondents, all but nine of the 516, stated that they had heard of "applications" on Facebook. However, there was a small percentage (around 2 percent) of respondents who consistently selected the "*I don't know what an application is*" answer when it was an option. This is understandable, as until mid-2010, Facebook did not offer on its website a definition of what an application was.

[6] http://www.facebook.com/press/info.php?statistics, read on June 3, 2011

[7] This group was based on correct answers to Questions 24, 26, 31, and 39, which can be found by question number in Appendix 7.

Most respondents (65 percent) had added fewer than 10 apps to their profile. A further 26 percent reported having added 10 to 15 apps, and only sixteen respondents stated having installed 50 or more apps. While the quantities of apps added are self-reported estimates, we know that all respondents had added at least one app: our survey.

Most respondents (76 percent) had removed at least one app in the past. This suggests that most respondents have some level of familiarity with Facebook's administrative controls for apps. However, next to the 14 percent who had not removed apps, 6 percent had wanted to but had not known how, and 4 percent were not sure whether they had removed an app or not. Three quarters of the respondents (74 percent) reported that they would remove an app from their profile after they have stopped using it.

In terms of the factors that influence the decision to add apps, less than half reported either only adding apps that their friends had added (46 percent) or only adding apps created by companies or people they had at least heard of before adding the app (42 percent). We also asked whether the respondents had read the "Allow Access" notice before they added the survey app to their profile. 44 percent responded that they had read it, 28 percent answered no, 25 percent stated that they had read the notice at some earlier time, and 3 percent could not recall whether they had read it or not.

4.2 Application Comprehension

When presented with knowledge-based questions about Facebook and apps, typically over half of respondents answered correctly. At the same time, on most questions there was a sizable group of respondents who selected "not sure"—often a greater part of the respondents than those who selected an incorrect answer.

Seventy-seven percent correctly answered a question about who creates apps (both FB and other parties), but almost a fifth thought that only parties external to Facebook create apps, and 4 percent stated they weren't sure. With our own survey app, 18 percent were not sure whether it was created by Facebook, even though the app explicitly stated its university affiliation. Forty-two percent of respondents correctly knew that Facebook does not review apps prior to publication, but a notable 48 percent weren't sure and 8 percent were under the mistaken belief that Facebook reviews the apps running on its platform.

When asked what it meant when the survey app needed to "pull" their information in order to work, 42 percent either answered wrong or were unsure.[8] While over half knew the right answer ("*"Pulling" means your profile data is transferred from Facebook's website to the survey application's website*"), the number of users who misunderstand application data exchange or are unsure of how it works is substantial. Similar confusion and uncertainty existed around whose information an can access; only 47 percent correctly answered that when installing an app that none of one's friends have added earlier, the app gains access not only to the user's profile information but also to the basic profile information of their Facebook friends.

Other questions attempted to measure how well users understood what profile data the survey app itself was allowed to access. There were ten answer options, as well as an all of the above or none of the above response, and the correct answer was a combination of seven of the options. The final score assigned partial credit for correct options and subtracted for incorrect options. This was a difficult question to answer considering this information wasn't readily available, and only one respondent identified all of the correct choices. The average score was 1.3 out of a possible 7. Over half (54 percent) selected "all of the above," which overestimates how much information apps can access. Given the complexity of answering this question correctly, it is not surprising that half of our respondents opted for this answer. It is regrettable that we did not include a "not sure" option for this question, as it could have captured more accurately whether or not respondents chose the "all of the above" answer because they believed it to be the case or that it was a convenient answer choice.

We asked a question about Facebook's privacy settings, too, where confusion and miscomprehension also prevailed. In response to the question "*Facebook recommends that you set some of your privacy settings to everyone*", 32 percent incorrectly believed that everyone stood for everyone on Facebook. While misunderstanding was widespread, most respondents (64 percent) correctly stated that everyone means "*everyone on the internet*."

4.3 Privacy Concerns Related to Facebook and Third-Party Applications

Concerning social networking sites in general, 36 percent somewhat or strongly agreed with a statement on interpersonal trust ("*I feel that I can trust other people on social networking sites with my personal information*"). The level of agreement was lower (28 percent of the respondents) when it comes to institutional trust ("*Social networking sites are run by companies I trust with my personal information.*").

When it comes to Facebook specifically, 80 percent of the respondents were very or somewhat concerned with the idea of Facebook selling their profile information to advertisers or other companies, whereas only 31 percent were equally concerned about immediate social threats on Facebook, such as parents or employers viewing their content or the posting or tagging of embarrassing photos of them by others.

Finally, we asked about information sharing practices that are explicitly prohibited by Facebook's Terms of Service (TOS) As we noted earlier, some companies were discovered engaging in these practices. However, due to Facebook's liberal user data sharing model and light oversight, it is possible that other app developers (especially those with less concern with the implications of violating Facebook's TOS or operating under less legitimate circumstances) are engaging in these activities. Over 90 percent of our respondents were very or somewhat uncomfortable with all of the three practices we asked about: an app selling their profile information, storing the information permanently on its own servers, or sharing their data with other companies.

5. BIVARIATE AND MULTIVARIATE ANALYSIS

We were interested in exploring the relationship between respondents' knowledge and behavior (e.g., usage) of third-party apps and their privacy attitudes in three areas: towards privacy-risky practices by third party apps, towards interpersonal privacy risks on Facebook (e.g., from other users), and institutional

[8] As mentioned earlier, this notice has since changed; the "pull" term has been removed, and the notice now lists the profile fields that the app will access.

privacy risks (e.g. by the company). Would more privacy-concerned respondents across these three dimensions demonstrate any differences in their knowledge or behavior? Also, we wanted to focus on the behavior and attitudes of the most knowledgeable group of respondents; given their expertise, would they behave or differ attitudinally from the less knowledgeable respondents?

We first examined these key relationships in the survey data using bivariate analysis. Then, we used regression analysis to examine the independent effects of five groups of independent variables. We review the bivariate findings briefly and the regression analysis in depth.

5.1 Bivariate Analysis

For our bivariate analysis, we created contingency tables using chi-squared tests of significance and t-tests to compare means when appropriate. Statistically significant relationships ($p<.05$) are discussed. Tables identifying all of the significant relationships are available in Appendix 5. Below, we highlight a few of the themes briefly.

5.1.1 Application Knowledge

A lack of understanding about the basics of how applications operate on Platform was correlated across multiple questions. Respondents who did not understand who makes apps (i.e., not limited to Facebook or only third parties) were also more likely to not understand whose profile information apps have access to when one adds an app (e.g., friends' profiles), and were less knowledgeable about what aspects of their own profiles apps could access. Respondents who incorrectly indicated that Facebook created our app were also highly likely to think that Facebook reviewed apps and to misunderstand whose profile data apps can access. Respondents who didn't understand what occurred when apps "pulled" profile information were also more likely to think that Facebook reviewed apps.

5.1.2 Experience With Applications

Experience with using applications (i.e., behavior) correlated with one's knowledge of how they function. For example, subjects who reported having removed an app from their profile were more knowledgeable about who makes apps, what profile information apps have access to, and were more likely to understand that Facebook doesn't review apps. This finding was bolstered when we performed categorical comparisons between our most knowledgeable respondents and the less knowledgeable. The most knowledgeable group engaged in all of the aforementioned behaviors at significantly higher levels.

Selectivity appeared to be related to privacy attitudes. Respondents who were selective about how they chose apps (i.e., only adding apps from people or companies that they had heard of before), were also slightly more concerned about issues of institutional privacy, and also had significantly less information in their profiles (as measured by our calculation of the amount of information in respondents' profiles).

5.1.3 Privacy Attitudes and Applications

Our findings across the different aspects of privacy attitudes we measured were also internally consistent. Concerns with how applications handled personal information, concerns about Facebook's institutional privacy practices, and social (or interpersonal) privacy threats on social networks were all associated. The respondents who were more comfortable with apps sharing their profile information or storing it permanently had greater feelings of control over their personal information on social networks. They had more trust in how other social network members treated their profile information, and they evinced greater trust in the companies that own social networking sites.

There were some relationships to other third-party app questions when making comparisons with our Facebook-specific privacy variables. When examining respondents' attitudes towards institutional privacy, greater concern was associated with adding fewer apps, while those who showed little concern were more likely to incorrectly believe that our app was created by Facebook.

5.2 Regression Analysis

We identified four dependent variables to examine. Three were privacy focused: respondent concerns about information disclosure by applications, Facebook institutional privacy concerns, and social threats to privacy. The fourth variable was the respondent's status as most or least knowledgeable about third-party apps. We used ordinal logistic regression to analyze the privacy variables in order to preserve the ordered, categorical status of these variables, and logistic regression for the most knowledgeable variable to capture the dichotomous comparison between two groups. We report the likelihood ratios, probabilities, and pseudo R^2 values appropriate for logistic regression models in Appendices 1-4.

We examined the effects of five groupings of independent variables on our dependent variables. Group One included demographic variables (gender, age, education) and whether or not a respondent was on the authors' friends list. Group Two included general social networking site variables: did respondents belong to other SNSs, how often they reported visiting SNSs, and how many adverse privacy events they may have experienced on SNSs. The number of adverse privacy events was calculated as a count of positive responses to several possible privacy-related incidents; e.g., *"Have you ever been embarrassed by information you shared or that was posted about you on a social networking site?"* Group Three included specific aspects of Facebook usage related to information disclosure and privacy that were separate from using the application platform: how much data respondents' profiles contained, whether or not they understood the term "everyone" as used by Facebook in their privacy settings, and whether or not they used Facebook Connect. Groups Four and Five consisted of third-party app behavior and third-party app knowledge questions respectively, with the exception that when we tested the most knowledgeable dependent variable, we removed the redundant knowledge questions from Group Five and added the three dependent privacy variables (as independents) as an additional group.

We created three nested models to explore these effects. Model 1 incorporated Groups 1-3; Model 2 added Group Four; and Model 3 added Group Five (and Six for the most knowledgeable). We interpret the results at a significance level of $p\leq.05$, but because we were not testing specific hypotheses we include a correction for the effects of multiple testing (using a Bonferroni adjustment). This is a conservative approach that increases our confidence that results that meet this threshold are not spurious (given that in a model with many variables some may be significant by chance), but may in fact eliminate some relationships that are in fact significant.

5.2.1 Information Disclosure by Applications

Our third-party app privacy variable was a composite of the three questions we asked about information disclosure practices by

apps: one's level of comfort if an app sold their profile information, stored their profile information permanently on its website, or shared their profile information with other companies. We calculated the mean across each question to create a composite measure (α = .89); the distribution of responses was not normal and skewed towards discomfort with these practices. Interestingly, none of the application-related covariates had any significant association with this measure. All three models revealed that adverse privacy events have a significant influence on application disclosure attitudes, with higher levels of concern associated with more adverse privacy events (M1: $p \leq .01$, M2-M3 $p \leq .05$). Use of Facebook Connect is negatively associated with this measure; Connect users are more likely to be less concerned with these practices (M2-3: $p \leq .05$). However, after conservatively adjusting the *p*-value threshold to correct for multiple testing to $p \leq .002$, none of these results were significant.

5.2.2 Facebook Institutional Privacy

To measure respondents' concern with issues of institutional privacy (e.g., actions undertaken by the company rather than by other members), we asked the respondents about their level of concern should Facebook ever choose to sell their profile information to advertisers or other companies. Responses move from low to high concern. The distribution of responses was not normal but skewed towards high concern. The adverse privacy events measure was a significant positive influence on institutional privacy attitudes, too, across all three models, with higher adverse privacy events scores associated with higher levels of concern ($p \leq .001$). This finding holds after adjusting for multiple testing. While none of the behavioral variables was significant, one knowledge variable was: if respondents answered correctly to our question asking if the survey application was created by Facebook ($p \leq .01$). There was a negative association: incorrect answers were associated with higher levels of concern. However, this finding did not withstand the correction for multiple testing ($p \leq .002$).

5.2.3 Facebook Interpersonal Privacy

As privacy issues on social networks are most often discussed in terms of interpersonal risks, rather than institutional ones, we asked respondents about their level of concern with three specific social privacy threats: "*My parents or other family members viewing my profile information or photos of me that might concern or offend them*," "*Current or future employers viewing my profile or photos of me*," and "*Embarrassing photos of me posted or tagged by others.*" We calculated the mean across each question to create a composite measure (α = .80); responses were normally distributed, and concern levels moved from low to high.

This was the only privacy variable to have a statistically significant demographic covariate—age—and it was significant across all three models, though it only withstood the correction for multiple testing *(*$p \leq .002$) in Model 1 ($p \leq .001$). The coefficient is negative, and age decreases as concerns increase about social threats to privacy. Like the institutional privacy variable, adverse privacy events are a significant predictor across all three models; the coefficient is positive, with the number of adverse privacy events increasing with concern levels ($p \leq .001$). This finding holds after adjusting for multiple testing. Membership on additional social networking sites (M1-3: $p \leq .05$), M2: $p \leq .01$), as well as installing a higher number of applications (M2: $p \leq .01$, M3: $p \leq .05$), was associated with higher concern, but did not withstand the multiple testing threshold. No knowledge-related covariates were significant.

5.2.4 Most Knowledgeable Respondents

Gender and education were significant across all three models when examining the most knowledgeable respondents: as the raw numbers foretold, this group was both predominantly male (despite the overall gender split of 60/40 women to men in the respondent pool; $p \leq .01$)) and highly educated ($p \leq .05$). The most knowledgeable respondents were also more likely to be on the author's friends list ($p \leq .05$). While adverse privacy events and membership in other social networking sites were both significant in Model 2 ($p \leq .05$ for both variables), these effects disappear in the full model (Model 3). After correcting for the effects of multiple testing ($p \leq .03$), only the gender and friends list covariates remain significant in Model 3. None of the privacy attitudes or behavior variables was significant.

6. DISCUSSION

Third-party applications are a common feature of the Facebook experience, yet many of our respondents didn't understand how apps obtain and use their profile data or even what profile data apps can access. Additionally, the vast majority of our respondents reacted negatively to behaviors some app developers have engaged in—including distributing Facebook user IDs to other companies—despite violating Facebook's Terms of Service. Taken together, these results indicate that apps present a problem for managing users' privacy.

6.1 Summary of Findings

The bivariate comparisons demonstrated that our measures of knowledge, behavior, and privacy attitudes were internally consistent. We also identified associations between privacy attitudes and app usage behavior as well as between privacy attitudes and app knowledge, but these associations were not significant in our regression analysis. Interestingly, the only factor that was consistently predictive of every form of users' privacy concerns was having experienced an adverse privacy event on a social networking site. Though this finding is weakened when holding third-party app privacy attitudes to the conservative Bonferroni adjustment, given that it is still significant with our other two privacy dependent variables we suspect the finding is not spurious. One explanation as to why it does not withstand the multiple testing correction may be that responses to this question were highly skewed towards discomfort with these practices, and thus any factor would have needed to be highly significant to overcome this overwhelming response. Neither knowledge of app privacy practices nor behavior with apps was consistent with concerns about third-party apps. This finding suggests that people may base their concerns on concrete and personal understandings of risk, as opposed to general knowledge.

An interesting and unexpected result is the lack of any predictors associated with third-party app privacy attitudes after correcting the *p*-values for multiple testing. This suggests a few alternatives in addition to the non-normal distribution of responses: First, it is possible that the questions we used to measure this concept, despite having a high alpha, did not accurately reflect how users conceive of privacy with respect to third-party apps. The measure only asks about users' concerns about practices that are against Facebook's Terms of Service. This means that, for instance, the potential interpersonal privacy concerns related to apps were not included in our measure. Second, given the novelty and complexity of the application landscape, there may be too little awareness or general comprehension of what apps are, how they work and the kinds of threats they may pose to privacy that

answering questions about related concerns would be meaningful for users. Third, despite the number of factors we attempted to control for, it is possible we did not accurately identify factors that predict these attitudes.

Another finding from our analysis is an observed lack of correlation between privacy concern and behavior. A potential explanation for this discrepancy is that users have a broad misunderstanding of information disclosure practices on social networking sites, and users with different levels of knowledge weren't differentiated in previous survey-based research. Since knowledge seems like a reasonable predictor of rational behavior, as demonstrated by other studies [6,7], users' lack of comprehension about Facebook's application information-sharing model could explain the concern-behavior gap. This, however, was not upheld by the results of our analysis.

Finally, scrutinizing our most knowledgeable users yields some additional insights. Our most knowledgeable were also our most educated respondents, and they were overwhelmingly male—the only instance where gender was a significant coefficient. They were also more likely to appear on the authors' friends list; though we did not attempt to measure technical prowess in this survey, given our personal associations it is likely this group is more tech-savvy than the general public, and thus more familiar with how apps share information. But increased knowledge was not predictive of privacy attitudes and behaviors. Interestingly, adverse privacy events were significant with these respondents only in Model 2 when we included their app behavior; the effect wasn't present in either Models 1 or 3. While this group represents our "ideal" in terms of knowledge, as these respondents understand the information exchange between apps and the Platform, their usage and their privacy attitudes are no different from less knowledgeable users.

6.2 Design Implications

6.2.1 Adverse Privacy Events

The most consistent factor that correlates with increased user privacy concern in our study is the experience of an adverse privacy event on a social networking site. This suggests that informing a user about privacy practices and risks may not be enough to motivate change. Many users learn about privacy risks the "hard way," by experiencing first-hand an unwanted information disclosure event.

While designing systems that violate users' privacy in order to increase their level of privacy concern is obviously unethical, there are several examples of technologies that demonstrate the concrete rather than the abstract privacy risks associated with a technology. For instance, Firesheep is a browser extension that allows users to easily hijack a web session from another user on an insecure Wi-Fi network. [9] Although the privacy risk of insecure Wi-Fi has be understood for some time, Firesheep allows users to experience the risk firsthand. Similarly, the visualization of the iPhone's surreptitious location tracking files demonstrated a known privacy risk in a way that was highly visible and personal. [10] Both of these technologies were widely reported in the media even though the privacy risks were not new. Our study suggests that users may be more cautious about the privacy risks of apps if they have seen a concrete example of how their information could be used inappropriately.

6.2.2 Comprehending Third-party Apps

A substantial number of users don't understand how apps work, what information they can access, and how they are authored and reviewed. This suggests that as long as applications are given wide latitude to access user data, Facebook and other application platforms should consider ways of making that information more explicit, digestible, and actionable. Warning messages and privacy policies do not appear to be effective, as users in our survey who had read these statements neither knew more, acted different, or felt more concerned about apps than users who had not reported reading these statements.[11]

However, while it is fair to attribute some of the incomprehension and confusion around apps to poor communication on the part of Facebook, another challenge that makes apps difficult to understand is their complex information sharing model that does not fit with traditional understandings of how websites function. As it exists today (and at the time this data was collected), the Facebook Platform presents apps to users in an interface that suggests they are tightly integrated into Facebook's website. This is a substantively different experience from, for example, installing third-party software on a computer, and more like a co-branded experience, where a website integrates content or tools from a third-party into their existing site. The difference is that in the co-branded experience, one expects that some level of due-diligence has occurred; contracts have been negotiated, agreements signed, and the third-party has been vetted in some degree by the host in order to avoid damage to their reputation should something go awry. In the world of Facebook applications, this is not the case. Information about app authorship and stewardship—especially the lack of vetting and weak contractual obligations—should be clear to users if they are required to perform due diligence on behalf of the company.

6.2.3 Social Feedback

Another result with design implications is the association between interpersonal privacy concerns and the number of apps installed, though this result should be read conservatively as the result ultimately did not meet the multiple testing threshold. Yet it suggests that people may choose to install apps based on their privacy concerns about how these apps will disclose data on their profile and friends as opposed to the privacy concerns about disclosing their personal data to the apps. This supports the research by Besmer et al. [3] demonstrating that users see apps as tools for social interaction and are generally unaware or unconcerned about the potential for institutional privacy violations. Similarly, Kolesnikova et al. [12] showed that privacy concerns and perceived enjoyment are factors in determining disclosure.

Apps are rarely used merely for disclosing information—they are usually games, quizzes, or other forms of entertainment, and the information disclosure to the application is merely a by-product from the user's perspective. By increasing the enjoyment associated with accepting and using the app, the "privacy calculus" equation may change to cause users to be more likely to

[9] http://codebutler.com/firesheep

[10] http://petewarden.github.com/iPhoneTracker/

[11] We asked respondents whether they recalled reading the notice that appears when adding an app, as well as Facebook's own privacy policy.

share information that they would not be normally disposed to sharing. Effectively presenting the social nature of apps along with their institutional privacy risk remains a challenge for the HCI community.

6.3 Future Research

One direction for future research is the role and nature of adverse privacy events in shaping users' privacy concerns and behavior. Our study did not examine these events in depth. However, given that they were correlated with privacy concern, they may represent fertile ground for a study that examines what adverse privacy events are, what different effects they have on users, and how they can be brought to bear in the design of technology that supports user privacy.

Another area for further research is to determine what kinds of interactions support user understanding about privacy, and whether this understanding effectively changes behavior. For instance, Kelley et al. [11] show that simplified privacy statements can improve users' accuracy and enjoyment. However, they did not attempt to determine whether this improvement contributes to changes in actual information behavior disclosure. If institutional threats (that are prominently displayed in these privacy policies) have little effect on user behavior, then a statement that discloses social risks may be more effective in helping users make disclosure decisions.

Our study also suggests consideration of the effect of social feedback on privacy decisions. Debatin [10] showed that users overestimate the privacy risk of others and underestimate their own privacy risk, while Lewis [14] found that users are more likely to have a private profile if their friends have private profiles. Besmer's [4] application warning message makes social cues a primary indicator, but not all users are influenced by these cues. Understanding what role these mechanisms can play in privacy design could lead to better risk analysis and decision making by users.

7. CONCLUSION

Information exchange practices between Facebook Platform and its apps have received a tremendous amount of scrutiny and criticism, yet most Facebook users continue to use them. We discovered that many users have limited comprehension of the privacy issues posed by apps on Facebook Platform. Many users not only do not understand fundamental issues related to information disclosure in apps, but there was also a sizable number of respondents that, when asked, responded that they were "not sure," caught between misinformation and uncertainty.

Despite the confusion and false understandings, there was often a majority of users who did answer many of our knowledge questions correctly, and a minority that demonstrated superior knowledge. However, neither knowledge about how applications exchanged profile information nor behavior related to app usage was not a predictor of privacy concern. In sum, we were not able to establish a reliable relationship between privacy concerns and how people understand and use applications with on social networks. Instead, adverse privacy events on social networking sites were a more reliable predictor of privacy attitudes, indicating that finding a way to make privacy choices and their ramifications more personal and concrete may hold promise for future designs.

As the role of social networking sites becomes increasingly prominent in day-to-day online communications, so do the concerns about the privacy of the information their users disclose. Services such as Facebook straddle a fine line between helping users connect and share information with others while preventing them from unintentionally exposing sensitive or embarrassing information to other users or to third-parties. Facebook Platform allows app developers to build services that have access to a considerable amount of information about its users, and we think our work and the prior work of others demonstrates that users may enter into this new relationship without accurate expectations or a clear paradigm to guide them about how their personal data will be managed. The tight integration of the app platform into Facebook's service contributes to this confusion.

Finally, the interleaving of applications into social relations—apps are no longer just a useful tool or a game, but often a social experience—diverts attention away from the underlying institutional privacy concerns. The way apps are framed as entertainment and a social experience, combined with the obfuscation of the information exchange, make it unsurprising that users continue to farm online and shoot virtual bad guys with abandon.

8. ACKNOWLEDGMENTS

We wish to thank Joshua Gomez, Travis Pinnick, Andrew McDiarmid, Matt Earp, Jennifer Stoll, and Dan Turner for their assistance at various stages of this study. We give eternal gratitude to Coye Cheshire for his feedback. We thank Antti Oulasvirta, Saara Matala, Laura Kainulainen & Vilma Lehtinen for their helpful comments.

9. REFERENCES

[1] Acquisti, A. and Gross, R. 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. Proceedings of 6th Workshop on Privacy Enhancing Technologies (2006).

[2] Barnes, S.B. 2006. A privacy paradox: Social networking in the United States. First Monday. 11, 9 (2006), 11–15.

[3] Besmer, A. and Lipford, H.R. 2010. Users' (mis)conceptions of social applications. Proceedings of Graphics Interface 2010 (Toronto, Ont., Canada, Canada, 2010), 63–70.

[4] Besmer, A., Lipford, H.R., Shehab, M. and Cheek, G. 2009. Social applications: exploring a more secure framework. Proceedings of the 5th Symposium on Usable Privacy and Security (New York, NY, USA, 2009), 2:1–2:10.

[5] Besmer, A., Watson, J. and Lipford, H.R. 2010. The impact of social navigation on privacy policy configuration. Proceedings of the Sixth Symposium on Usable Privacy and Security (New York, NY, USA, 2010), 7:1–7:10.

[6] boyd, d. and Hargittai, E. 2010. Facebook privacy settings: Who cares? First Monday; Volume 15, Number 8 - 2 August 2010. (2010).

[7] Cain, J., Scott, D. and Akers, P. 2009. Pharmacy students' Facebook activity and opinions regarding accountability and e-professionalism. American Journal of Pharmaceutical Education. 73, 6 (Oct. 2009), 104.

[8] Christofides, E., Muise, A. and Desmarais, S. 2009. Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? CyberPsychology & Behavior. 12, 3 (2009), 341-345.

[9] Conti, G. and Sobiesk, E. 2007. An honest man has nothing to fear: user perceptions on web-based information

disclosure. Proceedings of the 3rd symposium on Usable privacy and security (New York, NY, USA, 2007), 112–121.

[10] Debatin, B., Lovejoy, J.P., Horn, A.K. and Hughes, B.N. 2009. Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. Journal of Computer-Mediated Communication. 15, 1 (2009), 83-108.

[11] Kelley, P.G., Bresee, J., Cranor, L.F. and Reeder, R. 2009. A "nutrition label" for privacy. Proceedings of the 5th Symposium on Usable Privacy and Security (New York, NY, USA, 2009), 4:1–4:12.

[12] Kolesnikova, E., Gunther, O. and Krasnova, H. 2009. "It Won't Happen To Me!": Self-Disclosure in Online Social Networks. AMCIS 2009 Proceedings. (Jan. 2009).

[13] Krasnova, H., Gunther, O., Spiekermann, S. and Koroleva, K. 2009. Privacy concerns and identity in online social networks. Identity in the Information Society. 2, 1 (2009), 39-63.

[14] Lewis, K., Kaufman, J. and Christakis, N. 2008. The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. Journal of Computer-Mediated Communication. 14, 1 (2008), 79-100.

[15] McCarthy, Caroline. 2009. Facebook app privacy: It's complicated. CNET.com. http://news.cnet.com/8301-13577_3-10420499-36.html. Accesssed: 3-11-2011.

[16] Raynes-Goldie, Katie. 2010. Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. First Monday; Volume 15, Number 1 - 4 January 2010. (2010).

[17] Steel, E. and Fowler, G. Facebook in Online Privacy Breach; Applications Transmitting Identifying Information, WSJ.com. http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html. Accessed: 12-13-2010.

[18] Stutzman, F., Capra, R. and Thompson, J. 2011. Factors mediating disclosure in social network sites. Computers in Human Behavior. 27, 1 (2011), 590-598.

[19] Tufekci, Z. 2008. Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. Bulletin of Science, Technology & Society. 28, 1 (2008), 20 -36.

[20] Westin, A. 2001. Opinion surveys: What consumers have to say about information privacy. Prepared Witness Testimony, The House Committee on Energy and Commerce, WJ Billy Tauzin, Chairman. (2001).

Appendix 1: Third-Party App Privacy Concerns - Ordinal Logistic Regression

Independent Variables	**Model 1**	**Model 2**	**Model 3**
Demographics			
Gender	–.29(.25)	–.37(.28)	–.33(.29)
Age	.01(.01)	–.01(.02)	–.01(.02)
Education	–.07(.12)	.01(.13)	.03(.14)
On authors' friends list	–.01(.29)	–.10(.33)	.01(.33)
Social Networking Variables			
Do you belong to other social networking sites?	–.04(.27)	–.31(.32)	–.23(.33)
How often do you visit social networking sites?	–.04(.27)	–.46(.25)	–.46(.26)
Number of adverse events on social networking sites	.28(.10)**	.27(.11)*	.28(.12)*
Facebook Variables			
Amount of profile data	–.02(.02)	.00(.03)	–.01(.03)
Understands "everyone" in Facebook privacy settings‡	–.41(.25)	–.40(.28)	–.45(.29)
Uses Facebook Connect	–.49(.28)	–.66(.31)*	–.70(.32)*
Third-Party App Behaviors			
Number of applications		–.31(.27)	–.37(.27)
Removed application from profile		–.09(.52)	–.03(.54)
Discretion: only adds apps from people or companies they know		–.01(.15)	.03(.16)
Has clicked the "Leave Application" link when adding an app		–.20(.58)	–.13(.60)
Recalls reading the notice when adding an app		.34(.30)	.38(.30)
Third-Party App Knowledge			
What profile information can an app see? - correct responses‡			.07(.07)
Who creates applications?‡			.02(.36)
Was this application created by Facebook?‡			–.74(.40)
Does Facebook review apps?‡			–.17(.28)
Whose profile data can an app see when a friend adds an app?‡			–.11(.28)
What does it mean when an app needs to "pull" your profile information?‡			–.47(.29)
Log-likelihood	–282.86	–211.03	–216.09
Likelihood ratio x^2	22.630	27.63	37.51
Prob> x^2	.0122	.0240	.0147
Psuedo R^2	.0385	.0588	.0799

Note: coefficients are ordered log-odds, with standard errors in parentheses.

*$p \leq .05$ **$p \leq .01$ ***$p \leq .001$ †Significant after a Bonferroni correction for multiple testing ($p \leq .002$)

‡Indicates a question with a correct/incorrect response

Appendix 2: Facebook Interpersonal Privacy Concerns - Ordinal Logistic Regression

Independent Variables	Model 1	Model 2	Model 3
Demographics			
Gender	.08(.25)	.02(.28)	–.01(.28)
Age	–.05(.02)*** †	–.05(.02)**	–.05(.02)**
Education	.22(.19)	.17(.14)	.15(.14)
On authors' friends list	–.31(.30)	–.31(.34)	–.35(.35)
Social Networking Variables			
Do you belong to other social networking sites?	.59(.27)*	.64(.31)**	.66(.32)*
How often do you visit social networking sites?	.28(.19)	.10(.22)	.07(.22)
Number of adverse events on social networking sites	.58(.10)*** †	.63(.11)*** †	.63(.11)*** †
Facebook Variables			
Amount of profile data	–.06(.03)*	–.05(.03)	–.05(.03)
Understands "everyone" in Facebook privacy settings‡	–.30(.25)	–.19(.28)	–.23(29)
Uses Facebook Connect	–.12(.28)	–.52(.33)	–.53(.33)
Third-Party App Behaviors			
Number of applications		.67(.27)**	.65(.27)*
Removed application from profile		–.24(.49)	–.26(.50)
Discretion: only adds apps from people or companies they know		–.07(.15)	–.07(.16)
Has clicked the "Leave Application" link when adding an app		.24(.53)	.19(.54)
Recalls reading the notice when adding an app		.51(.29)	–.53(.30)
Third-Party App Knowledge			
What profile information can an app see? - correct responses‡			.01(.07)
Who creates applications?‡			–.09(.33)
Was this application created by Facebook?‡			–.21(.40)
Does Facebook review apps?‡			.08(.28)
Whose profile data can an app see when a friend adds an app?‡			.18(.27)
What does it mean when an app needs to "pull" your profile information?‡			.07(.29)
Log-likelihood	–295.45	–233.83	–233.33
Likelihood ratio x^2	72.81	68.47	69.47
Prob> x^2	.0000	.0000	.0000
Psuedo R^2	.1097	.1277	.1296

Note: coefficients are ordered log-odds, with standard errors in parentheses.

*$p \leq .05$ **$p \leq .01$ ***$p \leq .001$ †Significant after a Bonferroni correction for multiple testing ($p \leq .002$)

‡Indicates a question with a correct/incorrect response

Appendix 3: Facebook Institutional Privacy Concerns - Ordinal Logistic Regression

Independent Variables	Model 1	Model 2	Model 3
Demographics			
Gender	–.12(.23)	–.27(.26)	–.29(.27)
Age	–.01(.01)	–.01(.02)	–.01(.02)
Education	.06(.11)	.09(.13)	.09(.13)
On authors' friends list	–.10(.28)	.16(.31)	.26(.32)
Social Networking Variables			
Do you belong to other social networking sites?	.02(.26)	.09(.30)	.31(.31)
How often do you visit social networking sites?	.10(.16)	.13(.21)	.12(.21)
Number of adverse events on social networking sites	.32(.10)*** †	.36(.11)*** †	.37(.11)*** †
Facebook Variables			
Amount of profile data	–.02(.02)	.00(.03)	.00(.03)
Understands "everyone" in Facebook privacy settings‡	.12(.24)	.26(.26)	.22(.28)
Uses Facebook Connect	.06(.27)	–.03(.31)	.01(.31)
Third-Party App Behaviors			
Number of applications		–.37(.26)	–.41(.26)
Removed application from profile		.26(.47)	.27(.48)
Discretion: only adds apps from people or companies they know		.08(.15)	.11(.15)
Has clicked the "Leave Application" link when adding an app		.17(.54)	.20(.56)
Recalls reading the notice when adding an app		.41(.28)	.45(.29)
Third-Party App Knowledge			
What profile information can an app see? - correct responses‡			.01(.06)
Who creates applications?‡			.05(.33)
Was this application created by Facebook?‡			–1.23(.39)**
Does Facebook review apps?‡			–.05(.27)
Whose profile data can an app see when a friend adds an app?‡			–.07(.26)
What does it mean when an app needs to "pull" your profile information?‡			.05(.28)
Log-likelihood	–349.60	–277.42	–272.01
Likelihood ratio x^2	16.31	25.73	36.54
Prob> x^2	.0911	.0410	.0190
Psuedo R^2	.0228	.0443	.0629

Note: coefficients are ordered log-odds, with standard errors in parentheses.

*$p \leq .05$ **$p \leq .01$ ***$p \leq .001$ †Significant after a Bonferroni correction for multiple testing ($p \leq .002$)

‡Indicates a question with a correct/incorrect response

Appendix 4 – Most Knowledgeable Respondents - Logistic Regression

Independent Variables	Model 1	Model 2	Model 3
Demographics			
Gender	2.77(1.03)** †	2.95(1.23)** †	3.67(1.70)** †
Age	1.0(.02)	1.01(.03)	1.04(.04)
Education	1.69(.41)* †	1.69(.46)*	1.87(.56)*
On authors' friends list	1.94(.78)	2.44(1.08)* †	3.16(1.51)* †
Social Networking Variables			
Do you belong to other social networking sites?	3.94(2.51)* †	5.79(4.53)*	4.00(3.31)
How often do you visit social networking sites?	1.77(.71)	2.21(1.18)	4.67(4.82)
Number of adverse events on social networking sites	1.25(.17)	1.35(.21)*	1.35(.23)
Facebook Variables			
Amount of profile data	.95(.04)	.93(.04)	.91(.05)
Understands "everyone" in Facebook privacy settings‡	.57(.22)	.62(.27)	.49(.24)
Uses Facebook Connect	1.52(.64)	1.63(.78)	1.46(.79)
Third-Party App Behaviors			
Number of applications		.95(.41)	1.24(.60)
Removed application from profile		.97(.90)	1.75(2.10)
Discretion: only adds apps from people or companies they know		.90(.23)	.96(.28)
Recalls reading the notice when adding an app		.1.35(.66)	1.41(.77)
Third-Party App Knowledge			
What profile information can an app see? - correct responses‡			1.19(.12)
Who creates applications?‡			1.56(1.23)
Privacy Variables			
Third Party App Privacy Attitudes			.92(.34)
Facebook Institutional Privacy Attitudes			.88(.26)
Facebook Interpersonal Privacy Attitudes			1.07(.31)
Log-likelihood	–102.21	–81.66	–70.48
Likelihood ratio x^2	41.23	46.10	54.18
Prob> x^2	.0000	.0000	.0000
Psuedo R^2	.1679	.2201	.2776

Note: coefficients are ordered log-odds, with standard errors in parentheses.

*$p\leq.05$ **$p\leq.01$ ***$p\leq.001$ †Significant after a Bonferroni correction for multiple testing ($p\leq.03$)

‡Indicates a question with a correct/incorrect response

Appendix 5 – Bivariate Comparison Results

Independent Variables – significance values for chi-squared and t-tests reported at $p \leq .05$

	Third Party App Privacy	**Facebook Interpersonal Privacy**	**Facebook Institutional Privacy**	**Most Knowledgeable**
Number of apps (23)			0.011	
Who makes apps? (24)	0.055			
Read app notice (25)		0.026		
Pulling info (26)	0.004			
Clicked leave app link (28)				0.008
This app FB? (30)			0.002	0.000
Whose info can app see? (31)				
Q32 # Correct				0.033
Remove app after stopping (33a)				
Add apps people/companies (33b)		0.041		0.034
Add apps friends (33c)	0.000			
Removed an app (34)				0.011
Apps reviewed by FB (39)				0.000
App sells profile info (40a)			0.000	
App stores profile info (40b)			0.000	
App sells info to others (40c)		0.007	0.000	
Adverse Events Measure		0.000		0.009
Profile Completeness	0.039			
Who is everyone? Q1006_recoded				
Uses FB connect q1010_recoded	0.005			

Dependent Variables – significance values for chi-squared and t-tests reported at $p \leq .05$

Note: Variables with no associations were excluded.

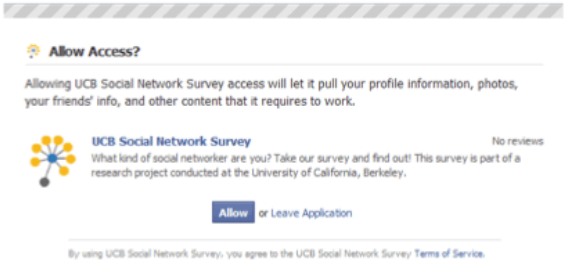
	Number of apps (23)	Who makes apps? (24)	Read app notice (25)	Pulling info (26)	Clicked leave app link (28)	This app FB? (30)	Whose info can app see? (31)	Q32 # Correct	Remove app after stopping (33a)	Add apps people / companies (33b)	Removed an app (34)	App sells profile info (40a)	App stores profile info (40b)	App sells info to others (40c)
Number of apps (23)	----													
Who makes apps? (24)		----												
Read app notice (25)			----											
Pulling info (26)	0.046			----										
Clicked leave app link (28)					----									
This app FB? (30)				0.012		----								
Whose info can app see? (31)	0.014	0.030				0.012	----							
Q32 # Correct					0.022		0.001	----						
Remove app after stopping (33a)			0.008						----					
Add apps people/companies (33b)	0.000								0.000	----				
Add apps friends (33c)									0.044	0.005				
Removed an app (34)					0.000		0.001		0.000		----			
Apps reviewed by FB (39)				0.047		0.001	0.001	0.018			0.001			
App sells profile info (40a)		0.017		0.015								----		
Adverse Events Measure														
Profile Completeness	0.019				0.005					0.003		0.005	0.002	0.040
Who is everyone? Q1006_recoded			0.039	0.005									0.002	

Appendix 6: Survey Questions

Third Party App Questions: General/Behavior	
22. Have you heard of "applications" or "apps" on Facebook?	
Yes	98% (504)
No	2% (9)
Not sure	0% (3)
23. Approximately how many applications have you added to your profile?	
Fewer than 10	65% (335)
10-50	26% (134)
50-100	2% (10)
More than 100	1% (6)
Not sure	4% (22)
I don't know what an application is	2% (9)
25. Did you read the "Allow Access" notice before you added this survey to your profile?	
Yes	44% (226)
No	28% (146)
I've read it before	25% (130)
I don't recall	3% (14)
28. Have you ever clicked the "leave application" link at this stage before adding an application?	
Yes	88% (454)
No	8% (41)
Not sure	4% (21)

33a. I'll remove an application from my profile after I've stopped using it	
Strongly disagree	5% (24)
Somewhat disagree	21% (101)
Somewhat agree	33% (160)
Strongly agree	41% (210)
33b. I only add applications created by people or companies that I've heard of before	
Strongly disagree	19% (92)
Somewhat disagree	39% (192)
Somewhat agree	27% (133)
Strongly agree	15% (72)
33c. I only add applications that my friends have added	
Strongly disagree	24% (113)
Somewhat disagree	31% (147)
Somewhat agree	38% (181)
Strongly agree	8% (39)
34. At least once I have removed an application from my profile	
Yes	76% (393)
No	14% (72)
I wanted to but was not sure how	6% (29)
Not sure	4% (19)
I don't know what an application is	1% (3)

Third-Party Application Questions: Knowledge	
24. Which of the following do you think is true about applications on Facebook?	
*Some are created by Facebook and some are created by people or companies other than Facebook	77% (397)
All are created by people or companies other than Facebook	17% (89)
Not sure	4% (22)
I don't know what an application is	2% (8)



26. The notice above tells you that this survey needs to "pull" your information in order to make it work. Which answer choice best matches your understanding of what this means?	
"Pulling" means the survey application is allowed to see your profile data but the data stays on the Facebook website	29% (151)
*"Pulling" means your profile data is transferred from Facebook's website to the survey application's website	59% (303)
None of the above - I think it means something else	2% (11)
Not sure	10% (51)

30. Was this application created by Facebook?	
Yes	1% (3)
No	81% (419)
Not sure	18% (94)
31. You decide to add an application to your profile that none of your friends have added to their profiles. Whose profile information can the application see?	
My profile info only	17% (89)
*My profile info and my friends' basic profile info	47% (240)
An application can access any Facebook user's basic profile information, whether they've added it to their profile or not.	8% (42)
None of the above	1% (7)
Not sure	27% (138)
39. All applications are reviewed by Facebook before you can use them	
True	8% (43)
False	42% (218)
Not sure	48% (250)
I don't know what an application is	1% (5)
32. Which parts of your Facebook account do you think this survey can access?	
Correct choices: Basic info, personal info, education/work info, groups, pages, friends list, photos	7 points possible
Incorrect: contact information, wall posts, messages, all of the above, none of the above	Mean: 1.56(2.11)
	0 correct: 55%
	1-2 correct: 17%
	3-4 correct: 10%
	5-6 correct: 19%
	7 correct: <1%

Third-Party Application Questions: Attitudes	
40a. How comfortable would you be with an application if it sold your profile information?	
Very uncomfortable	81% (419)
Somewhat uncomfortable	14% (73)
Somewhat comfortable	2% (8)
Very comfortable	3% (15)
40b. How comfortable would you be with an application if it stored your profile information permanently on its website?	
Very uncomfortable	60% (309)
Somewhat uncomfortable	30% (156)
Somewhat comfortable	7% (36)
Very comfortable	3% (14)
40c. How comfortable would you be with an application if it shared your profile information with other companies?	
Very uncomfortable	72% (373)
Somewhat uncomfortable	22% (113)
Somewhat comfortable	3% (15)
Very comfortable	3% (14)
16c. My parents or other family member viewing my profile information or photos of me that might concern or offend them	
Not at all concerned	44% (221)
Somewhat unconcerned	21% (107)
Somewhat concerned	29% (148)
Very concerned	6% (30)
16d. Current or future employers viewing my profile or photos of me	
Not at all concerned	32% (161)
Somewhat unconcerned	21% (106)
Somewhat concerned	34% (175)
Very concerned	13% (67)
16e. Embarrassing photos of me posted/tagged by others	
Not at all concerned	22% (109)
Somewhat unconcerned	24% (122)
Somewhat concerned	40% (200)
Very concerned	14% (70)

Facebook/General Questions	
1006. Facebook recommends that you set some of your privacy settings to everyone in order for people to find you more easily. What do you think everyone means?	
Everyone on Facebook	32% (167)
Everyone on my Friends List	1% (4)
Everyone on the internet	64% (332)
It means something else	.5% (2)
Not certain	2% (11)
1010. Some websites now have a feature that allows you to share what you do there (e.g. purchase movie tickets, or sign a petition) on your Facebook news feed. Do you ever use this feature to share your activities on other websites with Facebook?	
Yes	21% (106)
No	72% (372)
Not sure	7% (38)
16h. People have raised some issues specifically about Facebook. How do you feel about any of the following? Facebook selling my profile information to advertisers or other companies	
Not at all concerned	6% (32)
Somewhat unconcerned	13% (69)
Somewhat concerned	42% (214)
Very concerned	39% (199)