FACEBOOK AND USER-CONTROLLED PRIVACY: EVALUATING PRIVACY SETTINGS AS NOTICE-AND-CONSENT.

A Thesis
submitted to the Faculty of the
Graduate School of Arts and Sciences
of Georgetown University
in partial fulfillment of the requirements for the
degree of
Master of Arts
in Communication, Culture, and Technology

By

David G. Krone, B.S.F.S

Washington, DC
April 27, 2012

Copyright 2012 by David G. Krone
All Rights Reserved

FACEBOOK AND USER-CONTROLLED PRIVACY:
EVALUATING PRIVACY SETTINGS AS NOTICE-AND-CONSENT

David G. Krone, B.S.F.S.

Thesis Advisor: Mark MacCarthy, Ph.D.

ABSTRACT

Recently, organizations such as the Federal Trade Commission (FTC) have begun to enforce "notice-and-consent"—a privacy model that relies on users' ability to interpret an organization's written description of its information practices and to choose whether to participate. In the past, organizations using this model have fallen under harsh criticism for providing long, legalistic notices and confusing, unclear choices. Facebook has sought to address these issues through privacy settings such as the "inline" profile control. Ideally, these settings could vindicate notice-and-consent by using graphics, metrics and other mechanisms to better inform and facilitate privacy decisions. They are, however, new and untested. To evaluate these privacy settings for "notice-and-consent," therefore, I conducted a behavioral survey of Facebook users to determine the usability of these privacy settings and conflicts between users' setting selections and their privacy preferences. I hypothesized that the more usable a privacy setting is, the less it will be associated with privacy conflicts. I then tested these hypotheses using a multi-dimensional scaling and regression. I found that usability does reduce the rate of privacy conflicts, but the relationship is weak. However, highly visible settings, such as Facebook's "inline" profile and post controls, were associated with low rates of privacy conflict.

I would like to thank my advisors, Professor Owen and Professor MacCarthy, for their patience and guidance.

I would like to thank my family, Roger, Helen, Michael and Lauren, for their love and support. I would also like to thank Susie Kelly for her love and support throughout this process.

David G. Krone

TABLE OF CONTENTS

Introduction

From July 2009 to July 2011, the number of active users sharing personal information on Facebook tripled to over 750 million ("Timeline"). Users on Facebook and other sites, of course, do enjoy important benefits such as reconnecting with old friends or keeping up with current ones. As these sites grow, however, so does the concern that more and more of these users may be exposing their privacy online. In response, organizations like the Federal Trade Commission (FTC) have begun to enforce "notice-and-consent"—a privacy model that relies on users' ability to interpret an organization's written description of its information practices and to choose whether to participate. In the past, organizations using this model have fallen under harsh criticism for providing long, legalistic notices and confusing, unclear choices. Recently, websites such as Facebook has sought to address these issues through privacy settings such as "inline" profile controls. Ideally, these settings could potentially vindicate notice-and-consent by using graphics, metrics and other mechanisms to better inform and facilitate privacy decisions. They are, however, new and untested. The study, therefore, will evaluate the efficacy of these privacy settings for providing appropriate protection. In doing so, it will test their feasibility as a model for notice-and-consent.

Previously, privacy researchers and other advocates had intensely criticized the "notice-and-consent" model[a,b,c] for relying on long, vague and overly technical written privacy notices. Law Professor Fred Cate, for instance, warns these notices do not provide reasonable opportunity for choice and may result in only an illusion of privacy (Cate 343-344). A 2008 Carnegie Mellon study concluded users would have to spend 154 hours a year to even skim the policies for popular websites. Another study found these policies to be on a college reading level (Jensen 4). Even the choice of whether to consent may impede users. As Beales and Muris point out, notice and choice privacy regimes"…neglect the very real costs of processing information and making a decision" (Beales, Muris 113). If users are unable to understand the consequences of a privacy policy, their decisions may expose themselves to serious privacy harms.

Responses to these issues range from restricting certain uses of information to providing better mechanisms for notice-and-consent. Cate, along with Georgetown Professor Mark MacCarthy, advocate legislation that would eliminate certain risky practices as consumer options and regulate them purely on their potential to cause harm (Cate 370; MacCarthy 4). Perhaps more importantly, however, websites such as Facebook have focused on better informing and facilitating user choice through interactive tools ("Privacy Policy – Interactive Tools"). In 2009, for instance, Facebook launched the "Privacy Publisher tool." The idea was that when a user posts on Facebook, he or she could limit the post's audience using a drop-down menu embedded in the publishing tool itself. As Mark Zuckerberg commented, "The plan we've come up with

---

[a] For information on notice-and-consent generally, see "Privacy Online: Fair Information Practices in the Electronic Marketplace" (U.S. Federal Trade Commission, *Privacy Online)*.

[b] For information on notice-and-consent in financial privacy, see "In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act." (U.S. Federal Trade Commission, *In Brief*).

[c] For information on notice-and-consent in health privacy, see "Notice of Privacy Practices for Protected Health Information" (U.S. Department of Health and Human Services).

is… create a simpler model for privacy control where you can set content to be available to only your friends, friends of your friends, or everyone" ("An Open Letter"). By creating simpler, easier-to-understand privacy settings, Facebook could potentially reduce the risk of any number of its 750 million users exposing their personal information.

Likewise, many privacy advocates believe these tools could serve as more efficient methods of notice-and-consent. Stanford Professor Ryan Calo has praised Facebook's public profile as a form of "visceral" privacy notice. As he states, "experience can itself be a form of non-verbal notice, one that is substantially more efficient than language or symbols at creating in consumers an accurate mental model of a website" ("Facebook's New Privacy Tools"). Similarly, the Future of Privacy Forum conducted a study of behavioral advertising disclosures on websites. They concluded that a mix of graphic icons and longer disclosures could effectively communicate these privacy issues (Hastak, Culnan 2). A similar study concluded that these privacy indicators were particularly effective when well-timed and presented to users purchasing privacy-sensitive products (Egelman et al.). There is also some research that succinct and compelling notices do impact consumer behavior. Another Carnegie Mellon study in 2007 concluded, for instance, that users would pay a premium for products sold by a secure website (Tsai, Cranor and Acquisti 21-22). These studies indicate that, while there may be limits on the depth to which a user can understand a privacy policy, sites such as Facebook do have the opportunity to employ important mechanisms for facilitating users' control of privacy.

There are still major questions, however, on whether notice-and-consent compels users to appropriately protect their privacy. In 2011, for instance, a Colombia University study that analyzed Facebook user sharing practices determined that most users had not appropriately configured their privacy settings. As the study states, "every one of our 65 participants had at least one sharing violation based on their stated sharing intentions" (Madejski, Johnson, and Bellovin 14). Many users expressed that, in particular, they had not wished to share sexual content or content relating to alcohol. The study concluded that, although Facebook applied privacy settings based on publishing tool, users actually approached privacy in terms of which categories of content belonged in which social context. Similarly, a 2005 study conducted a survey on participants' attitudes towards privacy and how, in the past, participants released private information—such as a social security number or home address—in different contexts. The survey results indicated that, although participants, "displayed sophisticated privacy attitudes and a certain level of privacy-consistent behavior, their decision process seems affected by incomplete information, bounded rationality, and systematic psychological deviations from rationality" (Acquisti 6-9). Many participants concerned about privacy, for instance, signed up for loyalty cards or did not use encryption, email filters or even document shredders. This disparity between users' preferences and their actual preferences does appear to limit the extent to which sites such as Facebook can safely allow them privacy control.

In spite of these studies, there appears to have been less research conducted on how users currently interact with privacy settings that a site such as Facebook has already implemented and that users must deal with on a frequent basis. In 2011, Carnegie Mellon researchers did conduct a study on the usability of settings for opting out of online behavioral advertising, such as Internet Explorer's opt-out tool or an ad blocking application titled "Adblock Plus." The study concluded that many of the most predominant opt-out tools faced issues such as a lack of feedback,

confusing interfaces and poor communication overall. That being said, there are important reasons to study the privacy settings implemented on a site such as Facebook that actually collects user information. Facebook, in spite of its criticisms, did endeavor to create privacy settings that meet the needs of over 750 million users ("Timeline"). An examination of Facebook privacy settings could indicate not only considerations in designing an effective privacy tool but also in scaling it to serve large numbers of users. Google, for instance, already incorporated lessons from Facebook in its social network, Google+. As the International Business Times states, the social network application integrated, "many of Twitter and Facebook's best privacy features while ignoring their flaws" (Anderson). In particular, Google implemented a "circles" feature to restrict sharing to social groups. A study of how privacy settings impact notice-and-consent, therefore, could greatly benefit from Facebook's experience. In addition, the FTC has also required that Facebook establish a new privacy program that will address, "the design and implementation of reasonable controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those controls and procedure" (*In the Matter of Facebook, Inc., a corporation*). Obtaining a better understanding of how these privacy settings perform will be essential to holding Facebook accountable as it implements the new program.

Therefore, to study the impact of Facebook's privacy settings on notice-and-consent, I conducted a behavioral study of how Facebook users use these settings to understand their privacy risk and to make decisions based on personal preferences. The survey itself will consist of five sections. The first section will determine whether the Facebook member uses the "wall" format for their Facebook profile or the new, "timeline" format. The second section will test respondents' ability to use the privacy settings to protect against specific harms. The survey will present the respondents with a privacy issue and prompt them to choose the appropriate settings in response. One prompt might be: "Choose Facebook settings that would only allow friends to tag photos of you." The results could indicate whether the settings discourage certain kinds of protections, such as content sharing restrictions on Facebook. The third and fourth sections will examine how respondents currently apply their privacy preferences on Facebook. Respondents will begin by submitting their Facebook privacy settings via multiple choice answers. Respondents will then answer questions about their preferences for each privacy practice. This section will permit the study to compare users' opinion on the issues with how they actually selected their settings and will be an important indicator for evaluating Facebook's design of the privacy settings. Due to cognitive interference in having users both test and retrieve privacy settings, the third section will use a different participant group than the second. Finally, the fifth section will collect demographic information

The study has five primary hypotheses. The first is that the more usable a privacy setting is, the less Facebook members will use it to make privacy selections that conflict with their preferences. This hypothesis will address whether the "usability" of a privacy setting contributes to notice-and-consent. The second hypothesis is that "inline" privacy settings, such as the "inline profile control, will be more usable and be associated with fewer privacy conflicts than the other, menu-exclusive setting. This hypothesis will address the impact of Facebook's "inline" settings on notice-and-consent. The third hypothesis will examine how users interact with Facebook information practices that have no corresponding setting, such as Facebook's use of cookies.

This hypothesis will test whether a user concerned about these practices understands that no privacy setting address, for instance, social plugin cookies. The fourth hypothesis will examine how user's experience with Facebook impacts their capacity to use the site's privacy settings correctly. A user's "experience" will include number of years on Facebook, frequency of checking Facebook for updates and the frequency of the user posting content. The final hypothesis, moreover, will compare the impacts of the "wall" and "timeline" profile formats on the usability of privacy settings. Ultimately, I do discover that the "usability" of a privacy setting is associates with fewer "privacy conflicts," but the relationship is weak. The "inline" settings, however, had at least 20% fewer conflict rates each than other privacy settings in the study. These "inline" settings, therefore, may constitute a privacy "best practice" applicable to other websites such as Twitter.

The thesis itself consists of six chapters. In chapter one, I will provide the theoretical framework behind Facebook's privacy settings. In particular, I will examine the background behind the "notice-and-consent" explore the issues entities such as Facebook or the FTC have experienced implementing the model. In chapter two, I will review the related, behavioral research that could provide explanations for how users interact with privacy settings such as those on Facebook. Chapter three will cover the methodology used to construct the survey. In particular, this chapter will explain how the study selected privacy settings and information practices for the survey and how they represent Facebook's model of notice-and-consent. Chapter four will explain the hypotheses in detail. Chapter five will cover the statistical analysis of the survey results. The study will conduct a multi-dimension scale, for instance, to understand how high "usability" scores affect rates of privacy conflict. The study will also employ regression techniques to reveal trends between demographics and certain usage behaviors. Finally, chapter six will summarize the results and discuss how they could potentially impact privacy models in the future.

Chapter I
Theoretical Framework

In recent years, the "notice-and-consent" privacy framework has come under a great deal of doubt on whether or not it can navigate users though the often treacherous world of information privacy. Many users and privacy professionals, for instance, are fed up with the privacy notices, which they argue cannot convey enough information about an organization or its practices so that the user can make effective privacy decisions. Many support a "harms" framework that would regulate privacy based on the use of the information. However, developments in technology could alleviate many of the problems "notice-and-consent" has had with transparency. Recently, for instance, privacy settings developed by Facebook and Google provide users with unprecedented insights into their personal information. These settings, along with other privacy tools, could play an important role in helping organizations that collect personal information protect and reassure their user base.

Many privacy standards, including those proposed by the US government, incorporate transparency as an important policy recommendation or practice. Interpretations vary between standards, but these standards typically examine transparency as a value that supports an individual awareness both of the personal information collected about him or her and the ways that organizations process, use or share that information. In the 2008 memorandum, for instance, the Department of Homeland Security (DHS) listed transparency as one of its Fair Information Practices Principles, requiring that, the "DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII)" (U.S. Department of Homeland Security). This standard applies not only to the DHS, of course, but sub-agencies that also deal with citizen's personal information, such as the Transportation Security Administration (TSA). The idea, of course, is that, by informing citizens of how their information is handled, the government allows citizens to personally safeguard their information and protect their privacy rights.

The DHS report, of course, only gives a high-level perspective on transparency and only applies to a few, albeit important, government agencies. However, the FTC recently released a report entitled "Protecting Consumer Privacy in an Era of Rapid Change" that gives it a much broader scope and breaks it down into specific practices. The FTC report, for example, unlike the DHS memo, attempts to apply universally to both private and public sectors. As the report stated, it intends to, "guide policymakers and other stakeholders regarding best practices for consumer privacy" (1). The idea is to provide a framework that can examine the role of privacy throughout both the government and private organizations. The report does not provide as succinct a definition of transparency as the DHS. However, it does break down transparency in several core measures. The report, for instance, specially cites one transparency measure as, "providing consumers with reasonable access to their data" and relates it to allowing consumers to compare different companies' privacy practices (69). Another important measure, according to the report is to, "simplify consumer choice and to provide choice mechanisms in a prominent, relevant, and easily accessible place for consumers" (69). Finally, the report mentioned several other measures,

such as educating consumers about privacy practices or posting visible notices if privacy policies change. Organizations implement some of these measures better than others. By providing these measures, however, an organization could potentially provide the core benefit of transparency – allowing an individual to understand the information collected about him or her and how that information is handled.

These transparency measures, of course, correspond to the Fair Information Practices underlying "notice-and-consent" model that has dominated privacy policy for the past several decades. The "notice-and-consent" model revolves around providing the individual with a "notice" or announcement of privacy policies that allow users to choose whether or not to provide personal information. As the FTC report summarized, the notice-and-consent model requires that,

> "(1) businesses should provide notice of what information they collect from consumers and how they use it; (2) consumers should be given choice about how information collected from them may be used; (3) consumers should have access to data collected about them; and (4) businesses should take reasonable steps to ensure…security" (7).

Transparency as defined by the DHS and in the FTC report, of course, has only limited relevance to security. The FTC report's emphasis on consumer education appears to support the model's notice requirement. After all, the more education a user receives about privacy, the more he would be able to understand a notice or notice mechanism. Otherwise, the FTC's transparency measures for 'notice,' 'consumer choice,' and 'reasonable access,' do appear match perfectly with the "notice-and-consent" model's first three requirements.

The key link between these requirements and transparency, however, is that the ability of a user to read an organization's privacy notice and to choose whether or not to give consent is only meaningful if there is enough transparency for the user to understand and differentiate privacy practices. The FTC emphasizes 'access' as a way of countering information brokers who create, "individual consumer profiles of dossiers that consumers do not know about and cannot control" (*Protecting Consumer Privacy* 7*)*. Ideally, for instance, could verify what personal data the broker collects. Furthermore, an effective 'choice mechanism' could help users understand the consequences of their decision. Facebook users, for instance, can use a public preview tool to see what profile information the websites shows to the internet or even to specific individuals ("Searching for People"). The tool helps Facebook users decide whether their comfortable with the amount of information available to other people, whether they would prefer even more stringent privacy settings or even if they would like their information to be more visible. Privacy notices also help users understand the impact of their decisions, though they are usually written statements. Transparency is the core of the "notice-and-consent" model, and is essential to empowering users to make effective privacy decisions.

Many of the important criticisms of the "notice-and-consent" model, moreover, revolve around the failure of the model to provide this appropriate transparency and empower user choice. Indiana University Law Professor Fred Cate, for example, has been particularly critical of written privacy notices. As he states, "Notices are frequently meaningless because individuals do not see them or choose to ignore them, they are written in either vague or overly technical

language, or they present no meaningful opportunity for individual choice" (Cate 1). Cate argues that the burden of controlling one's privacy is too demanding for the vast majority of users. Many users, for instance, simply do not want to put sufficient thought into choosing privacy settings. Few users, moreover, would be willing to spend the time to read and understand the often confusing notices. Cate points out that organizations must write these notices as legally precise, but often complex and long-winded contracts. Likewise, Aleecia McDonald, a researcher at Carnegie Mellon University, concluded that an individual could potentially require around 244 hours a year in order to read through the privacy notices of commonly-visited websites ("The Cost of Reading" 560). The difficulties in reading these notices diminish the user's ability to make privacy decisions. A user who ignores the privacy notice may not realize, for instance, what personal information is and is not necessary for participation in organization. They may also miss out on important information such as the process for opting out. In response to these failures of transparency, critics such as Cate have proposed other models of privacy. Cate argues, for instance, that organizations should stop focusing on providing notices and create, "substantive restrictions on data processing designed to prevent specific harms" (2). According to him, a privacy policy should protect against the potential harms of certain privacy practices, regardless of individual user preference.

In spite of these criticisms, however, recent site applications, such as Google's privacy dashboard or Facebook's privacy settings, could provide users with potentially significant level of transparency in making their privacy decisions. Both websites still provide a formal privacy notice, of course. Google' privacy dashboard allows a user to survey the personal data Google has collected about him or her on a single web page. As the official Google blog states, "the Dashboard summarizes data for each product that you use (when signed in to your account) and provides you direct links to control your personal settings" (Whitten, Adan, and Mayer). This addresses, of course, the FTC's emphasis on information access. It provides a succinct, transparent way for a user to decide whether or not he is comfortable with the amount of information held by Google. Facebook, similarly, recently released tools allowing users to preview their public search profile, preview a profile based on friend categories, list applications holding access to their profile, download their information and even mock target an ad ("Interactive Tools"). Facebook also allows users to cater the visibility of their profile based on categories such as "friends" or "everyone" (Zuckerberg "An Open Letter"). The settings correspond with the 'choice mechanism' mentioned earlier. Users can make granular decisions regarding the visibility of their personal data. Moreover, they can quickly understand the exposure by previewing their profile or even targeting an ad. The idea, as Stanford researcher Ryan Calo argues, is that, "rather than tell people at length what your privacy practices may be, you show them what they really are… Experience can itself be a form of non-verbal notice, one that is substantially more efficient than language or symbols" ("Facebook's New Privacy Tools"). In stark contrast with the written privacy notice, these experiential and visual tools may entice users to sort through privacy settings. Under this kind of transparency, moreover, a model of notice-and-consent could potentially be feasible.

There is, of course, a delicate balance between privacy policies that allow for individual preference and those that prohibit certain harmful policies by default. Already, certain laws prevent a user from opting out of an information practice where their participation could help

protect against a major harm or benefit the public good. The Gramm-Leach-Bliley Act (GLBA), for example, normally allows users to opt-out of sharing personal information. However, the act does not allow opt-out in cases where information sharing will protect the confidentiality or security of consumer records or protect against fraud (15 USC). This restriction is important due to the sensitivity of financial information and its connection to crime. Websites or organizations such as Facebook, however, normally do not deal with those considerations and can afford to allow users a range of choice. The more choice users have the more that can customize the site or application to maximize the value of their experience. Georgetown Professor Mark MacCarthy describes a similar range of policy options. As he states, "At the one extreme, policy makers could require individualized notice, a default of no use of information and a difficult or costly opt-in process…At the other extreme, policy makers could allow a more relaxed notice and choice regime" (38-39). The more transparent a privacy practice is, the more likely it is a user can effectively decide to consent or not. Likewise, the less transparent a privacy practice is, the less a user can decide effectively and the more the user will have to rely on other, less flexible protections.

At the same time, however, if something like the technology behind these privacy policies changed, then it could also shift this delicate balance between 'user choice' and 'protection from harm.' The reason, of course, is that privacy in any given context is based on a number of factors or "information norms." In her book "Privacy in Context," Helen Nissenbaum lists four norms: contexts, actors, attributes and transmission principles (140). Furthermore, she explains, privacy is "a right to appropriate flow of personal information…The norms, which prescribe the flow of personal information in a given context, are a function of the types of information in question; the respective roles of the subject, the sender (who may be the subject), and the recipient of this information, and the principles under which the information is sent" (127). If actors—say, Facebook users—become accustomed to posting personal details online, for instance, then the privacy right has shifted. Likewise, a change in the technology or "transmission principles," such as the introduction of Facebook's privacy tools, could potentially shift privacy farther from 'protection from harm' and closer to 'user choice.' An ability to view and permanently delete photos from Facebook servers, for instance, could reduce a need for stringent data breach or blackmail protections. Of course, there will always be a need for 'protection from harm.' Transparency technologies, however, could help keep control in the hands of the user.

One possible counter-argument, of course, is that users may not have the time or will to sort through tools such as privacy dashboards any more than privacy notices. As Fred Cate also pointed out, "choice is often an annoyance or even a disservice to individuals. For example, the average credit report is updated four times a day in the United States. How many people want to be asked to consent each time?" (1). There is certainly a range of policy options between 'notice-and-consent' and 'protection from harm.' One option is to ensure that default privacy settings provide a substantial level of protection. In spite of this issue, however, transparency and 'notice-and-consent' could still play a vital and growing role in the privacy field. There are a variety of users out there who use their online personal information for variety of purposes. Some users, for example, put most of their private and professional lives on the web. To them it's a productive and effective way to keep tabs on their relationships and explore new opportunities. Other users,

however, may find privacy controls are an effective way to create distance between them and a repressive, judgmental society. ‘Protection from harm,’ safe as it may struggle to meet both needs. The flexibility transparency and “notice-and-consent”, however, could potentially meet both needs.

Chapter II
Literature Review

Facebook founder Mark Zuckerberg has stated that Facebook is still committed to privacy control and transparency ("Our Commitment"). To this end Facebook has implement privacy settings such as the "inline" profile and post controls. Facebook's other interests, however, compete with these commitments. In 2011, for example, Facebook earned nearly $3.8 billion from advertising—nearly 90% of its total revenue. In pursuit of better advertising, however, Facebook has launched programs such as "instant personalization" that may violate user expectations of privacy by sharing personal information with third party companies ("Facebook Privacy"). Likewise, Facebook's core functionality is to provide value by encouraging peer-to-peer interaction. Users who rely on the site's default privacy settings, however, could potentially share personal information with the rest of Facebook ("Facebook Privacy"). In response to these issues, both Facebook and privacy researchers have examined how solutions such as privacy settings could affect privacy models such as "notice-and-consent." Both Facebook and privacy researchers have foreseen a role for transparency tools to help educate users. Increasingly, however, privacy researchers have viewed privacy settings as a supplement to other privacy solutions, such as legislation or self-regulation.

Facebook has advocated for privacy policies such as "notice-and-consent" both through avenues such as public statements and actual tools such as the "inline" profile setting. Zuckerberg himself, for instance, has argued that the success of a social network like Facebook does depend on users' sense of privacy. As he states, if users, "could make their page private, they felt safe sharing with their friends online. Control was key… That's how Facebook became the world's biggest community online" ("Our Commitment"). Zuckerberg has also noted, of course, there is a tension between users' desires to both share and continually protect information such as an email address. Currently, he says, no system, "enables me to share my email address with you and then simultaneously lets me control who you share it" ("On Facebook"). In response to these challenges, Facebook has sought several varying approaches these tensions by releasing tools such as the "inline" settings, granular application controls and even improving the written privacy policy (Kelly; He; "Data Use Policy"). Moreover, Facebook does appear to have grounded these efforts in "notice-and-consent." In a 2009 blog post, for instance, Facebook Chief Privacy Officer Chris Kelly did state that effective privacy is grounded in the principles of "control," "simplicity" and "connection" (Kelly). Similar to "notice," for instance, "simplicity" indicates that users are more likely to understand and use tools that are simple. "Control", similar to "consent", indicates that the more users control the audience for information, the more comfortable they feel sharing. Finally, "connection" states that tools such as "profile preview" can help users balance their needs to share information and protect privacy.

Perhaps nowhere on Facebook have these principles of "control," "simplicity" and "connection" been as important as in the settings for peer-to-peer privacy. Although tools such as "profile preview" do help simplify users' task of assessing their privacy exposure, tools such as the "inline" privacy setting could allow users in-depth, granular control over exchanges ranging

from posts and photos to profile information. Recently, for instance, Facebook users have suffered increasing numbers of peer-related incidents. In 2007, the Pew Internet Forum found 6% of teenagers experienced an embarrassing photo posted on Facebook without permission (Lenhart). Likewise, in 2009, a Georgia high school controversially fired a teacher for posting a picture of herself with a glass of alcohol ("Did the Internet Kill Privacy?"). In response, Facebook has released several tools to address these issues. The most prominent of these is the "inline" publisher privacy setting. This tool allows a user to choose the audience as they are actually creating the post or publishing the photo. As the Electronic Frontier Foundation (EFF) explains, "if you only want your close friends to see a particular photo, or only your business colleagues to see a particular status update, you can do that — using a simple drop-down menu that lets you define who will see that piece of content" (Bankston "Facebook's New Privacy Changes"). The tool should both provide granular privacy control and be more accessible to users than, say, a separate settings page. Similarly, in August 2011, Facebook released settings such as the "profile tag review" and the "content tag review" that allow users to review photos content posted about them before it appears on his or her profile. Ideally, these settings could allow users to proactively defend their privacy. As Facebook Vice President Chris Cox stated, "you should never feel like stuff appears there (on your profile) that you don't want… The profile is getting some new tools that give you clearer, more consistent controls over how photos and posts get added to it." Finally, of course, Facebook has released other settings, such as "inline" profile controls that allow the user to protect information such as the user hometown or phone number. Ideally, of course, as users publish more and more personal information online, settings such as these enable users to potentially track and protect that content.

As of yet, there does not appear to have been a large amount of research into the actual usability of privacy controls. However, privacy researchers do appear to have come to a consensus that, although social network sites such as Facebook may offer tools for peer-to-peer privacy, most users still regularly expose potentially sensitive personal information. Several studies, for instance, have determined users regularly expose personal information through misconfigured privacy settings. As mentioned previously, a 2011 Colombia University study examined how Facebook users share potentially sensitive content such as photos or political views. As the study concludes, "93.8% of participants revealed some information that they did not want disclosed… On the other hand, we also note that 84.6% of participants are hiding information that they wish to share. In other words, the user interface design is working against the very purpose of online social networking" (Madejski, Johnson and Bellovin 11). Likewise, in 2005, Carnegie Mellon University (CMU) researcher Ralph Gross released a study evaluating the information available from CMU student profiles. It determined that nearly 87.8% of student profiles reveal their birth date, 39.9% list a phone number, and 50.8% listed a physical address (5). Finally a 2008 study at the University of North Carolina compared different models of privacy settings and noted that Facebook's settings require, "the user to become acquainted with the site and be aware of the existing social structure to understand potential impact of the privacy settings" (Lipford, Besmer and Watson 6). There have been a few studies that focus on how users interact with the tools. As also mentioned previously, in 2004, Acquisti released a study indicating user's privacy behavior suffered from a lack of information and bounded rationality ("Privacy and Rationality"). Similarly, CMU researcher Laura Brandimarte released a study in

2010 indicating that, whether or not the privacy settings protected personal data, their presence encourages users to share more. As she states, a setting such as Facebook's publisher control, "decreases individuals' privacy concerns and increases their willingness to publish sensitive information, even when the probability that strangers will access and use that information stays the same or, in fact, increases" (Brandimarte, Acquisti, and Loewenstein 1). Privacy settings are supposed to help users feel comfortable conversing with peers on sites such as Facebook. The problem is that users relying on ineffective or misconfigured tools may not understand the risk of exposure.

Users' inability to understand their privacy risk has also become increasingly important as sites such as Facebook share more and more information with third-party entities such as application owners, partner websites and advertisers. Facebook in particular has run into issues with sharing initiatives such as Beacon ("Facebook Privacy"). In response, the social network site has both offered users the ability to opt-out of these sharing initiatives and, perhaps just as importantly, it has released tools that could provide users transparency into what information is shared and with whom. In 2010, for instance, Facebook required applications such as Farmville to inform users which personal information it needs before users can authorize the app to run. Ideally, this would force users to consider the privacy concerns before accessing an app. As Facebook Chief Technology Officer Bret Taylor explains, "to access the private sections of your profile, the application has to explicitly ask for your permission… this new permissions box will pop up whenever you install a new application or first log in to an external website with your Facebook account." In addition, Facebook also provides an application privacy dashboard that lists the last time each application accessed each piece of information (Constine). Finally, although Facebook says it does not currently share user information with third-party advertisers, it does provide a tool demonstrating how advertisers target Facebook ads ("Interactive Tools"). As Stanford Law Professor Ryan Calo explains, the idea is to provide a "visceral" privacy notice that guides the user through the privacy implications. As he states, "experience can itself be a form of non-verbal notice… Facebook offers a unique new tool that lets users see exactly how ads are targeted by going through the motions of creating an ad themselves" ("Facebook's New Privacy Tools"). Third-party information sharing between entities such as Facebook or application owners usually occurs behind the scenes. Transparency tools such as these should enable users to hold these entities accountable.

That being said, many researchers have noted these tools appear to be falling short of "notice-and-consent." Alternatively, privacy advocates have recently begun to position data sharing transparency tools as part of a privacy regime that also includes solutions such as self-regulation or better legislation. In 2010, the Electronic Privacy Information Center (EPIC) criticized the Facebook's "instant personalization" program for opting users into sharing information with the social network's partner websites without consent. In particular, EPIC criticized the program's "opt-out" tool. As it states, "Facebook conceals users' ability to fully disable Instant Personalization. A user is required to go to each individual Facebook Page and click "Block Application" for each Facebook pre-approved website and application" (*In the Matter of Facebook, Inc.* 20). The effort involved in these changes could dissuade Facebook users from applying their privacy preferences. Likewise, EPIC has also criticized that Facebook's cookies share information about users' behavior on other websites without their

consent or awareness (*In the Matter of Facebook, Inc.* 22). The issue is not unusual. In 2010, privacy researcher Aleecia McDonald conducted a study on internet users' general perception of cookies. She concluded that users, "are unclear on important details like whether cookies may be combined with other data, what data is stored in cookies… and they are particularly unclear about laws and law enforcement" ("Beliefs and Behaviors" 27). McDonald criticized web browsers' user interfaces for convoluting users' ability to manage cookies. She also concluded, moreover, that most users did not have the education or insight to manage cookies. This gap could potentially make relying on a policy like "notice-and-consent" infeasible. As she states, "Most non-regulatory approaches require consumers to understand tradeoffs and to know enough to take whatever actions will enable their privacy preferences. At the current moment that seems unrealistic" (27). Tools such as an ad creation application are, of course, important for informing the user and contributing to notice-and-consent. In response to these issues, however, both McDonald and EPIC have called for new regulations and legislation on how sites such as Facebook use cookies and share information with third-party entities ("Footprints Near the Surf" 160; *In the Matter of Facebook, Inc.* 31-36).

Finally, in addition to peer-to-peer privacy and third-party information sharing, Facebook also continues to address its written "data use policy." The site has improved the written policy's design, but privacy advocates continue to note that the policy is long and inaccessible to users. Previously, of course, privacy advocates such as Fred Cate or Aleecia McDonald have long argued that the written policy is ineffective as a tool for "notice-and-consent" (Cate). In 2008, for instance, McDonald calculated that the opportunity cost for users to read the privacy policies for the 75 most popular websites would amount to $781 billion ("The Cost of Reading" 541). In addition to the full policy, however, Facebook has added a data use policy overview that provides brief summaries of "How advertising works" and "Sharing with other websites" (("Data Use Policy"). Facebook also formatted the overview as a "layered notice." Ideally, as an article by the Center for Information Policy Leadership explains, this format would provide, "condensed notice that contains all the key factors in a way that is easy to understand and is actionable, and a complete notice with all the legal requirements." However, in 2009 study, Carnegie Mellon researchers determined that the "layered" format did decrease the time users took to find information, but at the expense of accuracy (McDonald et al., "A Comparative Study" 14). Furthermore, a New York Times article noted the length of Facebook's data use policy has increased every year from 1,004 words in 2005 to, most recently, 5,830 words in 2010 (Bilton). Although Facebook's data use policy does appear to be a good reference for its privacy practices, it does not provide effective "notice-and-consent."

Recently, several standards bodies have issued regulations that apply to Facebook's privacy issues. In regards to third-party sharing, for instance, the Digital Advertising Alliance (DAA) released a publication on "Self-Regulatory Principles for Multi-Site Data" in November 2011. The publication holds DAA companies accountable to principle ranging from limitations on the collection of information to restrictions on use of "multi-site data" for employment eligbility. Perhaps more importantly, as part of its settlement with Facebook, the FTC recently required the social network to, among other requirements, establish and maintain a privacy program to address privacy risks and, every two years, to submit to "obtain independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the

requirements of the FTC order" (*Facebook Settles FTC Charges)*. These events suggest that the FTC and other regulatory entities are beginning to adopt an approach to privacy that includes transparency tools and regulation. As McDonald comments, it seems likely that the U.S. privacy regime will be a patchwork quilt of, "self-regulation based around privacy policies and FTC enforcement, plus new regulations, plus new legislation, plus a race between privacy enhancing technologies and privacy invading technologies" ("Footprints Near the Surf" 160). Understanding how users interact with privacy settings on sites such as Facebook could help determine how those tools fit into the emerging privacy regime.

Chapter III
Methodology

To examine "notice-and-consent" on Facebook, I examined users' interactions with two specific Facebook policies related to privacy – "privacy settings" and "information practices." Facebook has many policies relating to how individuals and entities access and share information. A "privacy setting," as the FTC defines it, includes "any control or setting provided by Respondent (Facebook) that allows a user to restrict which individuals or entities can access or view covered information" (*In the Matter of Facebook., a Corporation.* 3). On Facebook, for instance, a member will use the "Who can post on your Wall?" setting, located in the "Privacy Settings" menu, to determine whether "Friends" or "No one" can post on the user's Wall. Conversely, I will define an "information practice" as a mandatory Facebook policy that allows individuals or entities to access or view personal user information. The idea is that an information practice does not have a corresponding setting. Facebook, for instance, does not currently provide a setting that addresses "cookies" or "social plugins". However, as the American Civil Liberties Union (ACLU) points out, "cookies alert Facebook every time you visit a website that has a 'Like' button or other Facebook social plug-ins" (Conley). Determining whether users are aware of both information practices and privacy settings and how this awareness impacts their behavior is, of course, essential to understanding Facebook notice-and-consent. Therefore, in order to evaluate how these settings and information practices impact privacy on Facebook, the survey will collect information both on user understanding and privacy preference for information practices without corresponding settings and on usability and privacy conflicts for privacy settings. The survey will target 14 representative settings and practices selected in the "Selecting Privacy Settings and Information Practices" section.

I will evaluate "notice-and-consent" for privacy settings by using the concepts "usability" and "privacy conflict." The idea is that the more usable a privacy setting is, the more a user will make setting selections that do not conflict with his or her preferences. The concept of "usability" refers to Facebook members' capacity to correctly use a privacy setting to restrict who can access or view the information corresponding with the setting to specific individuals/entities. A difficult-to-use setting could deter users from customizing these restrictions. For the operational definition of "usability," I used the questions relating to privacy settings from the "Survey Part 2(1)" section below. "Usability," of course, only addresses the ease with which users interact with a setting. The concept of "Privacy Conflict," however, addresses whether the setting actually protects users' privacy. Conceptually, a "Privacy Conflict" refers to a discrepancy in the user's current setting selection where more individuals or entities can access or view personal information than the Facebook member would prefer. The concept is actually composed of two parts. A "current setting selection" refers to how the privacy setting option as user has selected. For instance, a user could choose either the "No One" or "Friends" selections for the "Who can post on your Wall?" setting. The operational definition for "setting selection" will include the setting-related questions from the "Survey Part 2(2)" section below.

Similarly, the conceptual definition for "privacy preference" refers to the specific individuals or entities that the Facebook member would prefer to be able to access or view the member's personal information. In the "Who can post on your Wall?" setting, for instance, a user may prefer the "No one" selection. The operational definition for "privacy preference" includes the setting-related questions from "Survey Part 3" below. A "privacy conflict" occurs, therefore, if the user's "current setting selection" is more public than the user's "privacy preference." For instance, if a user preferred that no one be able to post on his or her wall, then the selection of the "Friends" option for the "Who can post on your Wall?" setting would conflict with his or her preference.

The "understanding" and "privacy preference" concepts for information practices are similar to the concepts for privacy settings. The idea is that, under the "notice-and-consent" model, Facebook should provide sufficient notice so that a user who does not prefer an information practice understands that the practice has no corresponding privacy setting. Like with privacy settings, the concept for "privacy preference" refers to the specific individuals or entities that the Facebook member would prefer to be able to access or view the member's personal information. In this case, the operational definition for "privacy preference" will include the questions relating to information practices from "Survey Part 3" below. Moreover, like "usability," the conceptual definition for "understanding" refers to Facebook members' capacity to discern whether an information practice has no corresponding setting. Similarly, the operational definition for "understanding" includes the practice-related question from "Survey Part 2(1)" below. "Understanding" may indicate, for instance, that a user believes Facebook provides a privacy setting that address monitoring of user behavior via cookies or social plugins. If user does not prefer this monitoring, he or she could faces potential privacy risk by relying on protection the setting does not provide.

Selecting Privacy Settings and Information Practices

The survey, of course, cannot cover all of Facebook's privacy settings and information practices. In 2010, the New York Times estimated that, at the time, "To manage your privacy on Facebook, you will need to navigate through 50 settings with more than 170 options" (Gates). The survey, therefore, featured 14 representative settings and practices based on whether they sparked controversy among privacy entities such as the FTC, EPIC and the EFF, covered an otherwise unrepresented user information category in Facebook's "Data Use Policy" or otherwise dealt with a pressing privacy issue. The FTC' November 2011 settlement, for instance, charged Facebook with making "deceptive privacy claims" regarding the visibility of user's information to both friends' applications and the user's, the visibility of "friends lists" and profile information to the public, the sharing of user information with advertisers, keeping information after the user deleted his or her account, and other privacy setting issues (*Facebook Settles FTC Charges*). By addressing these issues, the survey could provide insight in whether they continue to present privacy risks for users. Likewise, the "Data Use Policy" summarizes the user information Facebook collects, including registration information, information the user shares on Facebook, information other members share about the user, etc.

Privacy Settings

After a review of which Facebook privacy settings appeared to be less transparent and involved the most sensitive personal information, I included the following questions for part 2(1).

How would you change your Facebook settings so that only your Facebook friends could see a post you made on your wall? Posting on one's wall or timeline is perhaps the most frequent and media-rich way users share personal information on Facebook. Facebook does provide several settings to protect users' posts, such as the "default privacy control" in the privacy menu or the "inline" setting in the post itself. As Facebook states, "The control for who can see each post will be right inline (the posting setting). For each audience, there is now an icon and label to help make it easier to understand and decide who you're sharing with" (Cox). In spite of this setting, it does appear many users' privacy violations involving their posts. In a 2011 study, for example, Columbia researchers in a 2011 found that every one of the 65 participants mistakenly shared or hid posts with alcohol, drug, explicit, sexual, religious or otherwise sensitive content (Madejski, Johnson and Bellovin 12). This question, therefore, could provide insight into whether the user's ability to understand and use settings such as "inline control" lead to these violations.

How would you change your Facebook settings so only your friends could see what other users post on your wall? For other users' posts on the user's wall, Facebook does provide an "inline" indicator that displays the visibility of the post. However, Facebook does not actually allow members to use the "inline" setting to adjust the visibility for others' posts on his or her wall / timeline. Instead, the user must pick the visibility from a pull-down list located in a "Privacy Settings" sub-menu. Like the previous question, this prompt will delineate whether the user understands how to protect his or her friends' posts. In addition, however, the question will provide insight into how a purely menu-based setting—the control for others' posts—compares with a setting that also employs an "inline" user interface.

How would you change your Facebook settings so that Facebook could not identify you in a friend's photo and suggest to the friend that he or she tag you? The "tag suggestion" setting itself simply highlights the user in his or her friends' photos and recommends that the friend tag them. Ideally, this setting helps the users' friends share photos related to the user. However, in order to create these suggestions, Facebook actually uses a "face recognition" technology to scan all users' and attempt to identify the subjects. As the Facebook Blog states, "When you or a friend upload new photos, we use face recognition software—similar to that found in many photo editing tools—to match your new photos to other photos you're tagged in" (Mitchell). This setting, of course, could potentially threaten the user's anonymity, both in social contexts and in others. For instance, as EPIC pointed out, "in Iran, government agents have posted pictures of political activists online and used "crowd-sourcing" to identify individuals" ("In Re Facebook"). Users cannot actually prevent Facebook from scanning photos. By disabling the setting, however, a user can prevent friends from confirming the results of those scans and remove an incentive to share potentially sensitive photos. The question, therefore, will provide insight into whether the user can address these issues.

How would you change your Facebook settings so only your Facebook friends could see Facebook profile information you've listed? (e.g. education, friends list,

relationship status, photos, etc.) Profile information, ranging from the relationship status or birthday to phone number or physical address, is perhaps a Facebook member's most personal information on Facebook. Facebook has provided another "inline" setting allowing users to protect the information. A member, for instance, would select visibility using a pull-down menus located next to each information type in the user's "Info" or "About" page (depending on whether he was using the Facebook wall or timeline format, respectively). Unlike posts, however, the user cannot access this "inline" setting on the Facebook wall or timeline pages. Potentially, users may not interact with their profile information as much as their posts and therefore may not be familiar with their profile information settings. This is a particular concern since, as previously mentioned, Facebook has set the default settings for profile data to "public." The question, therefore, will examine whether the user can protect this personal information.

How would you change your Facebook settings so that only your Facebook friends could see your friends list? Facebook members also use an "inline" pull-down menu to select the visibility of his or her "friends list." This one, of course, is located in the "friends list" page. The "friends list" question likewise examines users' interaction with an "inline control." However, many privacy advocates and researchers have also pointed out the sensitivity of a user's "friends list." In 2009, for example, MIT researcher found they could predict a user's sexual orientation based on that friends list. As the Boston Globe reports, "by looking at a person's online friends, they could predict whether the person was gay. They did this with a software program that looked at the gender and sexuality of a person's friends and, using statistical analysis, made a prediction" (Finin). The question, therefore, will examine whether the user is able to protect this piece of information in particular.

How would you change your Facebook settings so that internet users could not find your Facebook profile (including your profile picture and name) by searching on Google? A Facebook member, of course, already could potentially expose his or her profile to nearly the 900 million other members on the site ("Fact Sheet"). In order to enable Google, Bing and other public searches on members, however, Facebook has also created a "public search listing" visible to not just Facebook members, but anyone who has access to the internet. Facebook did address privacy concerns by creating a related setting that deletes the listing when disabled. However, at the bare minimum, the listing will show the member's name, profile picture, gender and network ("What is a Public Search Listing?"). Upon creating a test Facebook account, however, I found that Facebook had set the default visibility settings for profile information and wall or timeline posts to "public." The "public search" setting could potentially expose the user's Facebook account to anyone across the internet that searches for the user via Google or Bing or otherwise can find the URL for the public listing. Most of the survey questions have limited their scope to the user's control of privacy on Facebook. User's responses on this question, however, may not only provide insight into the user's ability to understand a setting, but may also reflect on his ability to manage his or her "digital footprint"—the total collection of information about him or her online.

How would you change your Facebook privacy settings so that the Facebook applications your friends use could not see your photos or your interests, even if your friends can? Many privacy advocates, of course, have specifically criticized the sharing of user information to friends' application. In the November 2011 settlement, for instance, the FTC

charged that this sharing violated Facebook privacy promises. As the FTC's press release states, "Facebook told users they could restrict sharing of data to limited audiences – for example with 'Friends Only.' In fact, selecting 'Friends Only' did not prevent their information from being shared with third-party applications their friends used" (*Facebook Settles FTC Charges*). Likewise, EPIC has also warned users that Facebook has set the default visibility settings to show all their information to friend's apps. As its website states, applications, "by default get much of the information about that user's friends and network members that the user can see… an individual that has never joined any applications will have their information sent to the third party application when their friends or associates in their networks join" ("Facebook Privacy"). The corresponding menu setting, moreover, includes 17 types of information, ranging from the user's photos to his or her family and relationships. The question specifies "photos" and "interests" to keep the user's response simple. However, perhaps the most important risk involved in this practice is that it is non-intuitive. Unlike, say, a post, there is no immediate notice that a friend's app has collected the user's information. Likewise, the friend's apps do not provide privacy policies indicating how the information could help or adversely impact the user. This question, therefore, will help examine if and how the user understanding the sharing of personal information with friends' apps.

How would you change your Facebook settings so that Facebook does not send information such as your name, friends list and user ID number to partner sites such as Bing or Rotten Tomatoes? Conversely, Facebook's "instant personalization" feature does allow designated "partner" sites such as Rotten Tomatoes to collect user information. Ideally, the information allows the partner site to customize a user's visit. As the Facebook "Data Use Policy" explains,

> "When you visit an instant personalization site, we provide the site with your User ID and your friend list (as well as your age range, locale, and gender)… The site can also access public information associated with any of the User IDs it receives, which it can use to make the site instantly personalized. For example, if the site is a music site, it can access your music interests to suggest songs you may like" ("How do I control who can see what's on my profile (timeline)?").

"Public information," of course, includes the Facebook member's name, profile picture, gender, network and any content such as posts or profile information the user designated as "public" ("How do I control who can see what's on my profile (timeline)?"). Perhaps even more importantly, however, the partner website could potentially associate Facebook information with the user's on-site browsing behavior. As the EFF points out, "instant Personalization inherently requires tracking" (Jaycox). Facebook does allow members to disable "instant personalization" using a menu setting. In addition, partner sites must agree to abide by certain privacy practices, including providing an "opt-in" choice on the user's first visit or deleting the user's information if he or she disables the setting. Nevertheless, the user could potentially share large amounts of personal and behavioral information to sites such as TripAdvisor or Scribd. The question, therefore, could provide insight into whether the user understands how to consent or not consent to this information practice.

How would you change your settings so that Facebook cannot give other companies permission to use your name and profile picture in ads that your friends see? Like "Instant Personalization," the "third-party social ads" setting permits Facebook to share user's name and profile picture with third-party companies. Oddly enough, however, Facebook does not currently share this information. As setting's description states, "Facebook does not give third party applications or ad networks the right to use your name or picture in ads. If we allow this in the future, the setting you choose will determine how your information is used" ("Facebook Ads"). This setting does seem deceptive, as it does not indicate when Facebook may share this information nor to which companies. Facebook also enabled the setting by default and placed it under the "Account Settings" menu instead of "Privacy Settings." The question, therefore, will examine whether users are aware of this setting and if they can find it.

Information Practices

After a review of which Facebook information practices appeared to be less transparent and involved the most sensitive personal information, the survey included the following questions for part 2(1). The correct answer for each question is "No Corresponding Setting."

How would you change your Facebook settings so only your friends could see your post on someone else's wall? Unlike in the other two questions addressing user posts, Facebook does not allow users to change the visibility of a post on another's Facebook wall or timeline. As indicated previously, only the wall or timeline's owner can adjust the setting. It appears, therefore, that Facebook has modeled the privacy of posts around the centralized Facebook wall / timeline. The user has strong control over the visibility of content on his or her own wall, but less over content published elsewhere. This question, therefore, could indicate whether users understand the restriction of his or her control over the privacy of posts.

How would you change your Facebook settings so you could prevent a friend from tagging you in their photos? When a Facebook member "tags" another user in a photo or other content, Facebook both uses the tagged member's name to create a link from the post to his or her profile and it attempts to publish that post on the tagged member's wall or timeline. These "tags," of course, could potentially violate the member's privacy by associating him or her with profane or otherwise undesirable content. Perhaps the most egregious example is the 2009 case where a Georgia high school fired a teacher due to a Facebook photo of herself with a glass of alcohol ("Did the Internet Kill Privacy"). A text post, moreover, that tags a user will feature the user's name in the message itself. Facebook does provide several tag-related privacy controls. The "profile review," for instance, allows the user to, "review posts friends tag you in before they appear on your timeline" ("Facebook Ads"). The setting does allow the user to prevent a tagged post or photo from appearing on his or her wall. The post, however, will still associate the member's name with any potentially objectionable content, and it will still appear on the poster's wall or timeline and on the poster's friends' newsfeeds. Facebook does allow users to manually remove a tag from others' posts, but only *after* the other user publishes it. A user, therefore, cannot actually prevent another user from tagging him or her.

These "tagging" privacy settings, of course, do seem complex. Facebook may limit these settings in order to encourage members to tag others in their posts. However, it is also a very

public platform where both misguided friends and cyber bullies could potentially humiliate a user. This question, therefore, will verify whether the user is able to understand these risks.

How would you change your Facebook settings so Facebook does not share your name, profile picture and Facebook ID number with organizations, celebrities and other entities that you have "liked"? A user cannot "like" a page without providing this information. Originally, a user listed his or her "interests" only as another type of text-based information. In 2010, Facebook implemented a new privacy practice that actually created a connection between the user's "interests" and entities he or she "liked" and the Facebook page for that interest or entity itself. Ideally, this connection helps users share interests and organizations, celebrities or other entities to share news or content. As the Facebook Help Center states, when a user "likes" a page, "you are making a connection. A story about your like will appear on your Wall (timeline) and may also appear in News Feed… Facebook Pages you like may post updates to your News Feed or send you messages" ("Like"). However, the organization, celebrity, etc. can also see the name, profile picture, Facebook ID and any other public information for the user who "liked" the Facebook page. This may be an important issue as, increasingly, online organizations or entities such as those with Facebook pages are compiling larger and large amounts of user marketing information. As the Wall Street Times reports, "Consumer tracking is the foundation of an online advertising economy that racked up $23 billion in ad spending last year (in 2009)" (Angwin). The questions in part 3, therefore, will present the default settings for each of the privacy practice in part 2(1) and ask the user's preference. Some users may value exchanging a "like" and public information for content or updates. The question, however, will examine whether users understand the exchange.

How would you change your settings so that, while you are logged into your Facebook account in one browser window or tab, Facebook does not record when you open a site with a Facebook "social plugin" in another window or tab? Facebook "social plugins," such as the one pictured below, have surprised many users by showing them friends' photos on non-Facebook websites. The plugins themselves do not actually provide information with these websites. However, in order to deliver these photos, Facebook does actually to create a record of the user's visit to that third-party website, As the Facebook Help Center states, when a user logged into Facebook goes "to a website with a Like button, we need to know who you are in order to show you what your Facebook friends have liked on that site. The data we receive includes your user ID, the website you're visiting, the date and time, and other browser-related information" ("What Information Does Facebook Get about Me"). The Help Center also states that, if the user is not logged in, Facebook still does record the website, the date and time, and the browser information. Facebook, therefore, could potentially monitor user behavior not only on its own website, but across the internet. Moreover, although a user could avoid these issues using tools such as a browser's "incognito" mode, Facebook does not allow users to control or tailor this practice. The question, therefore, examines whether this practice is transparent enough that the user realizes he or she does not have control.

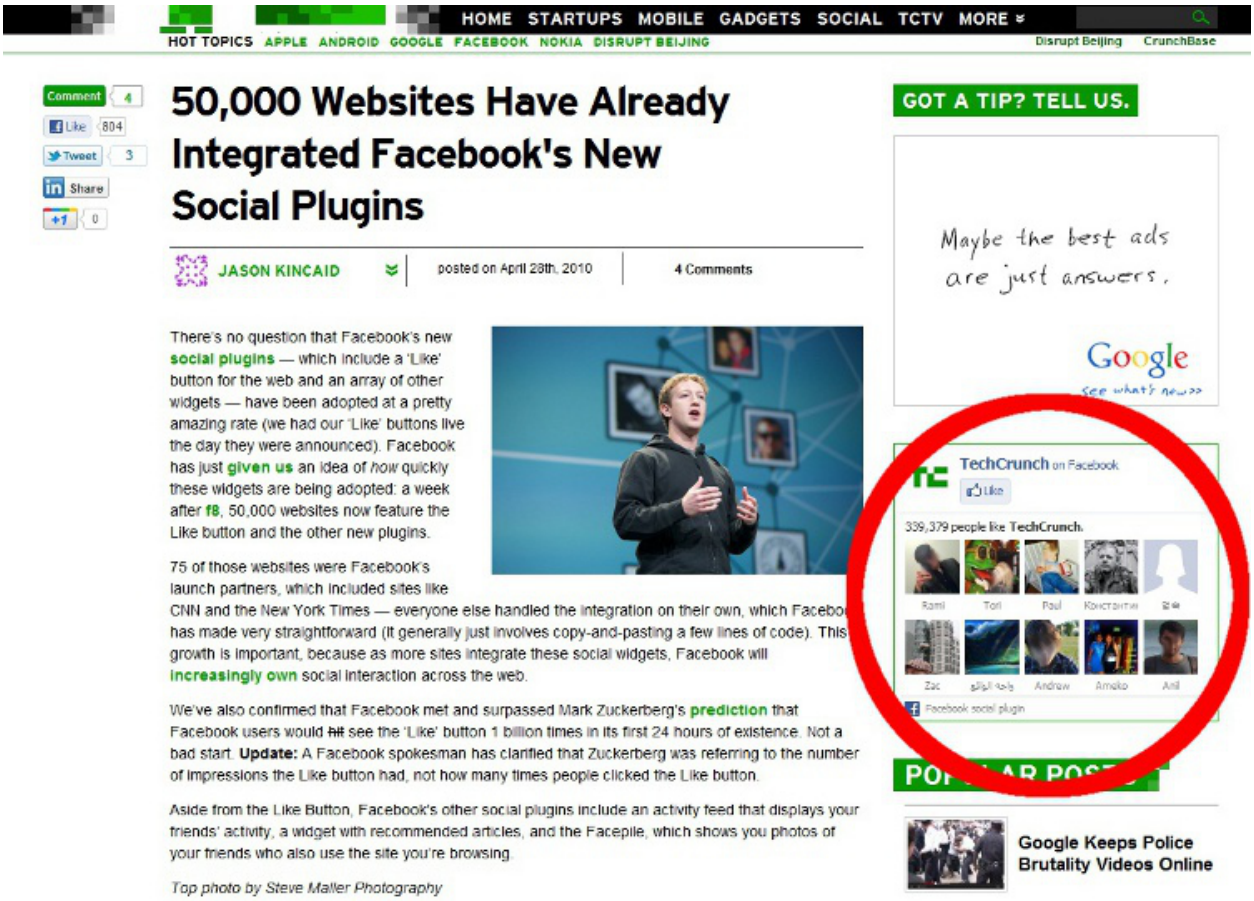

Fig. 3.1 A Facebook "social plugin" on Techcrunch.com

How would you permanently erase your Facebook account? Facebook members actually do have the option to permanently delete his or her Facebook account. Currently, however, a member would actually have to use the Facebook search bar in order to find the account deletion tool. The user could easily confuse the tool, however, with the one that temporarily "deactivate" the account, which is located in the user's "Account Settings" menu ("Security Settings"). As the EFF explains, "a deactivated account cannot be seen or found by others… Reactivating an account is done by logging in again with the same username and password. This means that all of the information that the user has uploaded is retained by Facebook" ("Facebook Privacy"). The question, therefore, will determine whether the user understands that "deactivating" an account does not erase it and whether the user can reasonably find the account deletion tool.

Technically, since account erasure does have a corresponding privacy tool, it could count as a "privacy setting" rather than an "information practice." Given that the tool would delete a user's account, however, the "Part 2(2) – Current Privacy Setting Selection" section of the survey could not determine whether users actually use the tool to close out accounts. Like an "information practice," therefore, I will only test whether the user can understand that the account deletion tool prevents Facebook from retaining closed account data.

Constructing the Survey

In order to examine these privacy settings and information practices, therefore, I constructed the Facebook privacy survey with the following sections:

Survey Part 1 – Timeline or Wall Format

In September 2011, Facebook began replacing the traditional "wall" format for the user's Facebook profile with the "timeline" format (Lessin). Although the change did add or eliminate privacy controls, it did change the URLs for pages such as the "Privacy Settings" menus. In addition, Facebook began rolling out the new format to only portions of the user population at a time. In order to accommodate users of both formats, part 1 asked the user to indicate which format his or her profile displayed. The survey used the answer to tailor several questions, such as displaying the correct picture for the "profile preview" question in part 2(1). The benchmark answers for part 2(1) also included separate answers for "timeline" and "wall" users if a settings' URL or location had changed. Perhaps, most importantly, the part 1 answer also allowed me to conduct a comparison between "wall" and "timeline" users in the analysis section.

Survey Part 2(1) – Privacy Setting Usability and Information Practice Understanding

Users may have expectations or prior knowledge about a Facebook privacy setting or information practice. While Facebook offers the same user interfaces to all its members, of course, examining how participants independently use these expectations to interact with Facebook's privacy controls is important to examining the "usability" of a privacy setting or "understanding" of a practice. Therefore, the questions in part 2(1) will both ask users to configure a setting according to a prompt and purposely give participants a free response field and a "No Corresponding Setting" option to record their answers. By not suggesting an answer, for instance, the free response field allows me to explicitly examine only expectations and knowledge the users currently hold. The field itself actually consists of two text boxes—one for the user to input the setting's webpage URL and the other to explain the setting itself. For example, a question may prompt the user to ensure only "friends of friends" can send friend requests. The user, in turn, may pick a setting he expects addresses this issue. He or she may also perform a Google search for "Facebook friend requests." Both answers should indicate how the user would respond to the privacy concern outside the survey. The survey, moreover, will score participants' abilities to use each setting by comparing their responses with pre-defined answers. For instance, to discern whether a user would be able to use the setting above, I will determine whether his response cited the "Who can send you friend requests?" menu at "facebook.com/ajax/settings/privacy/connect.php." For some settings, Facebook does users with multiple ways to adjust their privacy protection. For instance, a Facebook user could adjust the visibility of others' posts on his or her wall either by adjusting the "Who can see what others post on your timeline?" setting located at "facebook.com/ajax/settings/privacy/tag.php" or by using the "Limit the Audience for Past Posts" located at "facebook.com/settings/?tab=privacy." Either answer will count as demonstrating the setting's usability

Many advocates, of course, have criticized Facebook not only for unclear settings, but also for practices such as third-party information sharing that users do not have control over. The EFF noted, for example, that Facebook may track users on non-Facebook sites with "social plugins" without consent. As the EFF states, "just seeing the "like" button (on the "social plugin") is enough for Facebook to collect a record of your reading habits" (Jaycox). A user may believe that disabling or adjusting a Facebook setting would prevent the collection. Perhaps even more likely, users may not be aware that Facebook collects information about their behavior on other sites. Therefore, to examine users' understanding of practices that do not have a corresponding privacy setting—such as monitoring user behavior on other sites—the survey included a "No Corresponding Setting" checkbox as a response option. The checkbox should force participants to distinguish between Facebook privacy practices they do and do not control. The survey, of course, will include questions that address privacy practices without corresponding settings. Similar to questions about practices that do have settings, the survey will determine whether or not the participant understands a privacy practice—such as monitoring users via "social plugins"—by validating he or she checked the "No Corresponding Setting" option. The user response will provide insight into both whether they generally understand the scope of "consent"—their ability to disable or tailor privacy settings. It may also indicate whether the user has misconstrued a setting. For instance, the user may believe disabling the "social ads" setting prevents Facebook from collecting user information from "social plugins" on other sites. Likewise, a user may also underestimate privacy controls by choosing "No Corresponding Setting" for a question that does have a setting. In these cases, the user may not be aware of or may not be able to find the setting needed to protect his or her privacy.

The questions for part 2(2), therefore, had the following format:

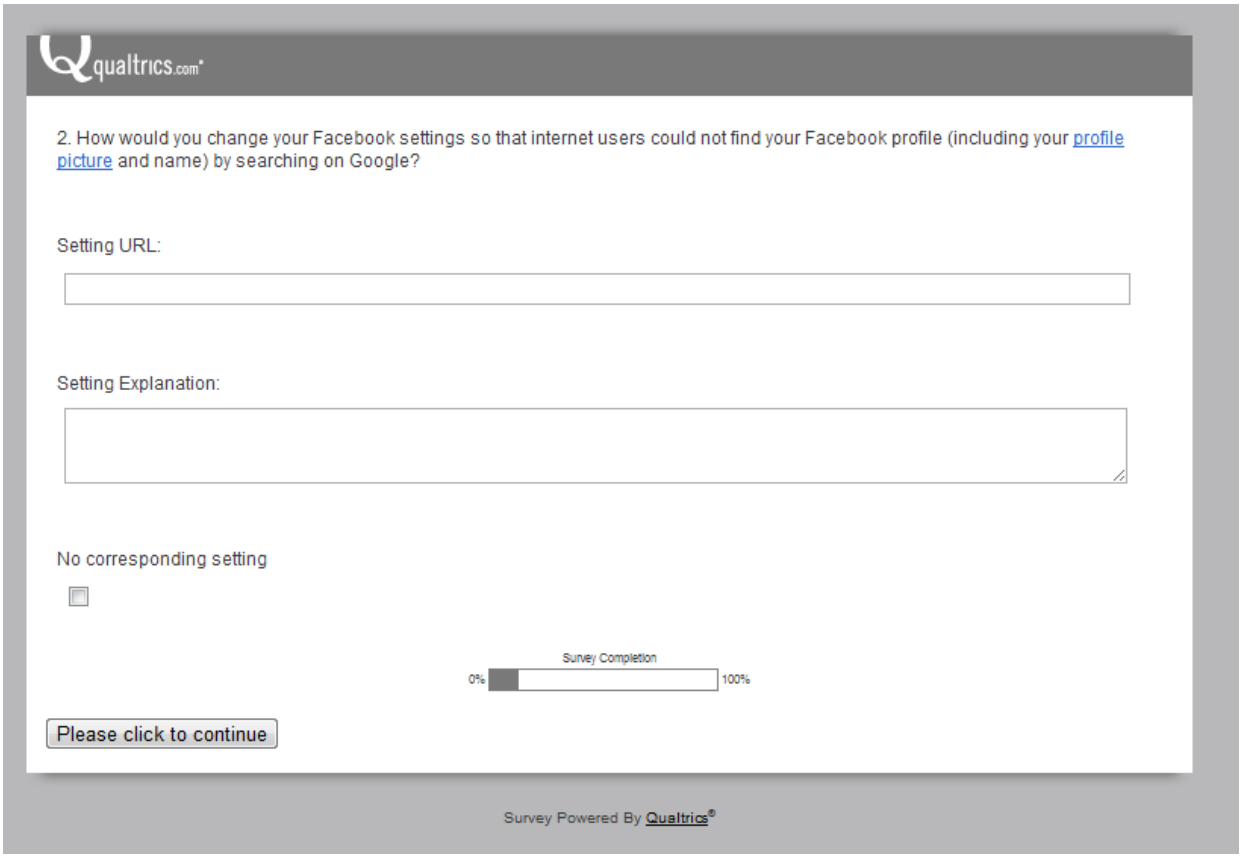

Fig. 3.2 Example question from part 2(1)

Part 2(2) – Current Privacy Setting Selection

To determine how users currently use Facebook privacy settings, therefore, the questions in part 2(2) ask users to report on their current settings for each of the privacy settings in the "Selecting Privacy Settings and Information Practices" section above. Although Facebook members may demonstrate they have the ability to correctly use a privacy setting, they may or may not actually interact with the setting outside of this survey. Participants may not be aware of a privacy issue or its corresponding privacy setting. The questions in part 2(2) do not include information practices, as they do not have corresponding privacy settings. In addition, the questions also approximate the language and the interface of the privacy settings as they appear on Facebook. For instance, one question asks "Who can see Wall posts on your profile?" This matches the language in the Facebook. Also like Facebook, the user chooses his or her response from a pull-down menu.

In addition I also split the survey participant population between parts 2(1) and 2(2). Unfortunately, many Facebook privacy menus do not have a "cancel" or "button." In a test surveys, I found that users would accidentally change their privacy settings when responding to prompts in part 2(1), changing the answers they would have had for questions regarding their current privacy settings in part 2(2). Moreover, conducting part 2(2) would reveal the answers to

part 2(1), invalidating the tests of user's understanding of privacy controls. All survey participants, however, took parts 1, 3 and 4.

Part 3 – Privacy Preferences

The questions in part 3, therefore, will present either the information practice itself or the default selections for each of the privacy settings and ask the user's preference. Of course, if the participants have not actually changed their privacy controls, the settings they report may only be the Facebook defaults. The user will respond by indicating they prefer or do not prefer the information practice or default selection, or that have no preference. To determine Facebook's default privacy setting selections, I created a new Facebook account and examined the corresponding settings from part 2(1). The defaults for privacy settings, therefore, came out to the following:

Privacy Setting	Default Selection
Visibility of users' posts on user's wall/timeline	Public
Visibility of other users' posts on user's wall/timeline	Public
Tag suggestions	Enabled
Profile information (e.g. education, relationship status)	Public
Friends list	Public
Public search listing	Enabled
Information types friends can bring to their applications	All possible types
Instant Personalization	Enabled
Visibility of third-party social ads	Friends

Table 3.1 Default Selections for Facebook Privacy Settings

Similarly, the policies for information practices are as follows:

Information Practice	Policy
Visibility of user's posts on other users' walls/timelines	Public
Other users can tag user in photo without permission	Enabled
"Liked" Facebook pages can see user's public information	Enabled
Facebook can monitor user behavior via "social plugins"	Enabled
Facebook saves user information after user closes account	Enabled*

*As discussed previously, users can choose between the "deletion" and "deactivation" to close their account. Since Facebook makes it difficult for users to find the "deletion" tool, I will count "deactivation" as the policy.

Table 3.2 Policies for Facebook Information Practices

Part 4 - Demographics

Finally, in part 4, the survey asks questions about the participant himself. These included questions covering basic demographic information such as gender, age, education and income. In addition, part 4 also asks about participants about their Facebook usage, such as the number of years the participant has had a Facebook account, how often the participants checks Facebook for updates on his or her news feed, wall comments, etc., and how often the participant posts on

his or her Facebook wall / timeline. These usage questions could indicate how users' engagement with Facebook affects their ability to understand privacy settings.

Survey Distribution

In order to test privacy setting "usability" and information practice "understanding," I needed a large, randomized population of internet users who would be willing to take the survey. To distribute the survey therefore, I used Amazon.com's crowd-sourcing service, Mechanical Turk. The service distributes tasks ranging from not only surveys but to audio transcriptions and website usability tests to users of the service in return for payment. Mechanical Turk is relatively new, but internet researchers have increasingly begun using the service to find large populations of internet users willing to participate in studies. As Carnegie Mellon researcher Patrick Kelley comments, until recently, studies involving internet users "were commonly advertised in an ad-hoc fashion, using mailing lists, contest sites, and online bulletin boards. Recently Amazon's Mechanical Turk, a service where users can complete short tasks and receive automatic payment, has become prominent" (Kelley 1).

I distributed my Facebook privacy survey, therefore, in two phases. The first phase did include all parts of the survey described above. However, due to an error the survey did not collect the current setting selection and the user preference information for the "profile information" and "visibility of user's posts on user's wall" settings. Therefore, I also launched a second phase of the survey that collected only the current selection and user preference information for those settings. Both surveys did use Mechanical Turk users as populations, so their results should be comparable. However, I examine the demographics for both surveys in the "Analysis" chapter below. For each survey response, moreover, I paid the user $1.37. The first survey resulted in a total of 885 responses. The second resulted in 400 responses.

Chapter IV
Hypotheses

Usability Hypothesis

The first hypothesis addresses "usability" of a privacy setting is in fact associated with lower rates of "privacy conflicts." Ideally, if settings such as "Who can look up your profile?" are effective at enabling privacy setting decisions, users should have made setting selections that correspond with their privacy preferences. This hypothesis compares, therefore, whether Facebook members are capable of correctly using a privacy setting with whether they actually use the setting to make selections that match their preferences. Given the examination of current setting selections, of course, the test of the hypothesis will not include information practices. The hypothesis is as follows:

H_1: The more usable a privacy setting is, the less likely it will be associated with privacy conflicts.

"Inline" Settings Hypotheses

The second category of hypotheses address the impact that "inline" setting design in has on privacy conflicts and usability. The "inline" settings include the ones for "profile information," "friends list," "visibility of user's posts on user's wall" and "visibility of others' posts on user's wall." The "visibility of others' posts" setting does not allow a user to make a setting selection in the post itself, but it does provide an indicator in the post stating its visibility. The analysis, therefore, will include it as an "inline" setting.

Facebook implemented these "inline" settings in 2011 to help simplify control over content such as users' wall/timeline posts, profile information and friends lists. As Facebook states, "Content on your profile, from your hometown to your latest photo album, will appear next to an icon and a drop-down menu. This inline menu lets you know who can see this part of your profile, and you can change it with one click" (Cox). Many privacy advocates, of course, lauded the settings as facilitating user choice. As EFF Senior Staff Attorney Kurt Opsahl commented, Facebook was "moving in a direction of providing more granular controls on profile posts… Giving people additional controls is good so long as those controls are understandable and easy to use" (Mills). In my survey, these are the only privacy controls that have a setting out side of Facebook menu. Therefore, to test these hypotheses, therefore, I will compare the "usability" and the "privacy conflict" between these "inline" settings and the remaining, menu-exclusive settings. The hypothesis, therefore, are as follows:

$H_{2A:}$ "Inline" settings are less likely to be associated with privacy conflicts than menu-exclusive settings.

$H_{2B:}$ "Inline" settings are more likely to be usable than menu-exclusive settings.

Information Practice Hypotheses

The third set of hypotheses address information practices on Facebook that do not have corresponding privacy settings. The risk, of course, is that without corresponding settings, Facebook does not provide sufficient notice about information practices, such as "monitoring via plugins." This hypothesis tests, therefore, whether users who are concerned about these information practices are able to understand that Facebook does perform these practices and that there are no corresponding settings. This test will compare whether those concerned are more likely to correctly answer the "understanding" question for each practice. The hypothesis, therefore, are as follows:

$H_{3A:}$ Users who do not prefer "tagging without permission" are more likely than users who do to understand the information practice has no corresponding setting.

$H_{3B:}$ Users who do not prefer "information sharing with 'Liked' entities" are more likely than users who do to understand the information practice has no corresponding setting.

$H_{3C:}$ Users who do not prefer the "visibility of users' posts on others' wall" are more likely than users who do to understand the information practice has no corresponding setting.

$H_{3D:}$ Users who do not prefer "monitoring via social plugins" are more likely than users who do to understand the information practice has no corresponding setting.

$H_{3E:}$ Users who do not prefer "retention of closed account data" are more likely than users who do to be capable of correctly using the "delete account" tool.

Facebook Experience Hypotheses

The first two sets of hypotheses tested Facebook "notice-and-consent" by comparing setting usability to user privacy conflicts. Those hypotheses examine whether users currently use settings to make privacy decisions. However, in order to examine the extent that users must be familiar with these settings to use them, the thesis will compare participant's ability with how often participants check Facebook, how often they post, and how long they have had an account. Ideally, for instance, the more experience has on Facebook, the more he or she should be able to use Facebook privacy settings or understand Facebook information practices. A user who frequently checks other users' walls/timelines or posts frequently himself may have become concerned about the availability of personal content and have familiarized himself with the settings. Similarly, a user who has spent years on Facebook would have had more opportunities to experience a privacy incident and seek out the corresponding setting. The hypotheses, therefore, are as follows:

$H4_{A1}$: The more often a user posts on his or her Facebook wall or timeline, the more likely the user will be capable of correctly using Facebook privacy settings or understanding information practices.

H_{4A2}: The more often a user checks for updates on their Facebook wall, timeline or newsfeed, the more likely the user will be capable of correctly using Facebook privacy settings or understanding information practices.

H_{4A3}: The more years a user has had a Facebook account, the more likely he will be capable of correctly using Facebook privacy settings or understanding information practices.

“Wall” and “Timeline” Hypotheses

Finally, privacy advocates such as the Electronic Privacy Information Center have criticized Facebook’s replacement of the Facebook “wall” with the new “timeline” format (“EPIC Urges FTC Investigation into Facebook Timeline”). The “timeline” format did move the locations of the “inline” privacy settings, such as the controls for user profile information. However, “timeline” did not appear to move the majority of the Facebook controls, and the new locations seem to be intuitive. The thesis, therefore, will test changes in privacy setting usability between the Facebook “wall” and “timeline” using the following hypotheses.

H_{5A}: Users that had the “timeline” format are less likely than users with the “wall” format to be capable of correctly using privacy settings and understanding information practices.

Chapter V
Analysis

Descriptive Statistics

In spite of its large, diverse user base, the Amazon Mechanical Turk website also appeals to certain demographics that appear to skew the population's descriptive statistics. The sample populations, both for survey 1 and 2, do appear represent most demographics appropriately. For instance, the sample populations for both the first and second surveys evenly represent a wide range of incomes. Likewise, the large majority of the surveys' respondents also have a bachelor's degree or some college education. The second survey's population, moreover, is split evenly between genders, with 205 male and 196 female respondents. The second survey population also represents Facebook "wall" and "timeline" users fairly evenly, with 182 and 219 respondents respectively. However, the populations for both surveys did skew towards respondents in their 50s, 60s and 70s. In addition, the population in the first survey skewed significantly towards female respondents and "timeline" users.

Nonetheless, these demographics should not adversely impact the analysis. Researchers, for instance, have noted that women are more likely than men to choose protective setting selections. A 2012 Pew Forum study noted, for instance, that "67% of female profile owners restrict access to friends only compared with 48% of male profile owners. Likewise, men are more apt than women to choose partially private (23% vs. 16%) or fully public (26% vs. 14%) settings" (Madden). A larger proportion of women, therefore, could provide more respondents who are actually concerned about their privacy settings. Moreover, in part 2(1) of the first survey for this thesis, 50.67% of males and 50.27% of females were able to correctly respond to the question prompts. The large number of female respondents, therefore, should not impact the analysis. In addition, researchers have also indicated that a respondent's age does not have a substantial impact on the privacy setting selections he or she chooses. As the Pew Forum again states, "users of all ages are equally likely to choose a private, semi-private or public setting for their profile. There are no significant variations across age groups" (Madden). Therefore, the surveys' disproportion in age should also not impact the analysis

Finally, Mechanical Turk users did take the survey as Facebook began replacing the "wall" format with "timeline" on a rolling basis. This timing does allow the analysis to compare the "wall" and "timeline" formats, but it was difficult to evenly represent both formats. The first survey, of course, took place three months earlier than the second, which explains why the second's population uses the two formats equally. As mentioned in the "Hypotheses," the "timeline" format does not appear to have significantly changed or rearranged the privacy controls. The hypotheses comparing the two formats should provide insight into their relative merits, but the separate formats should not impact the rest of the analysis.

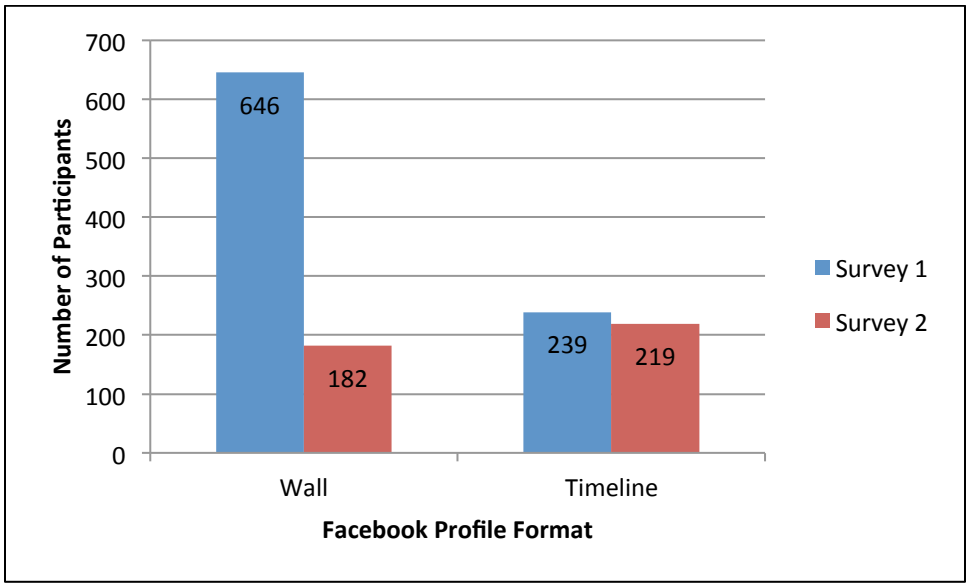

Fig. 6.1 Number of Survey Participants using "Timeline" or "Wall" Formats

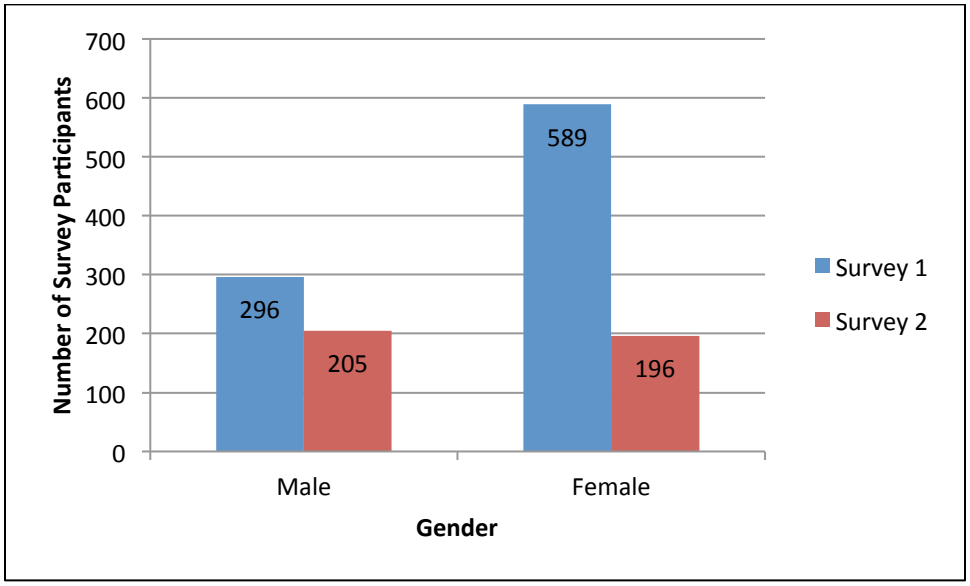

Fig. 6.2 Number of Male and Female Survey Participants

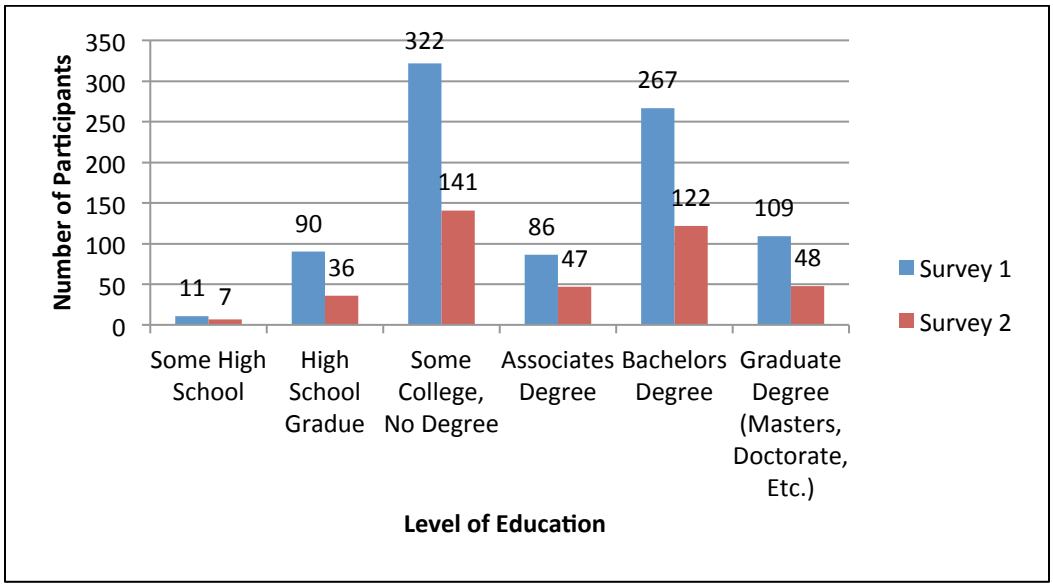

Fig. 6.3 Survey Participants' Education

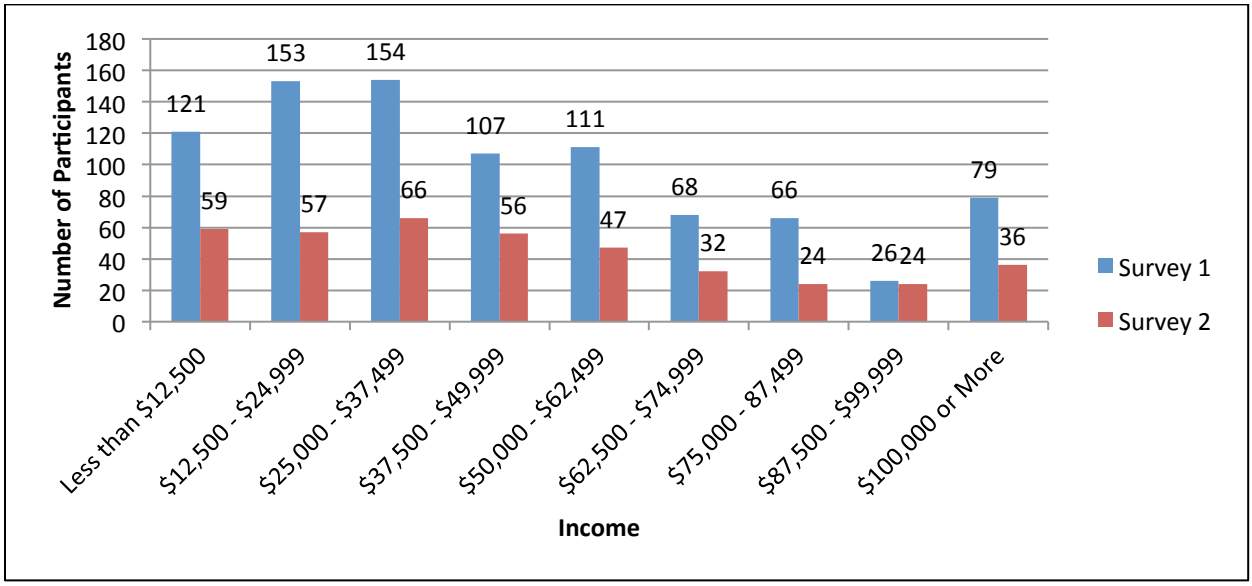

Fig. 6.4 Survey Participants' Income

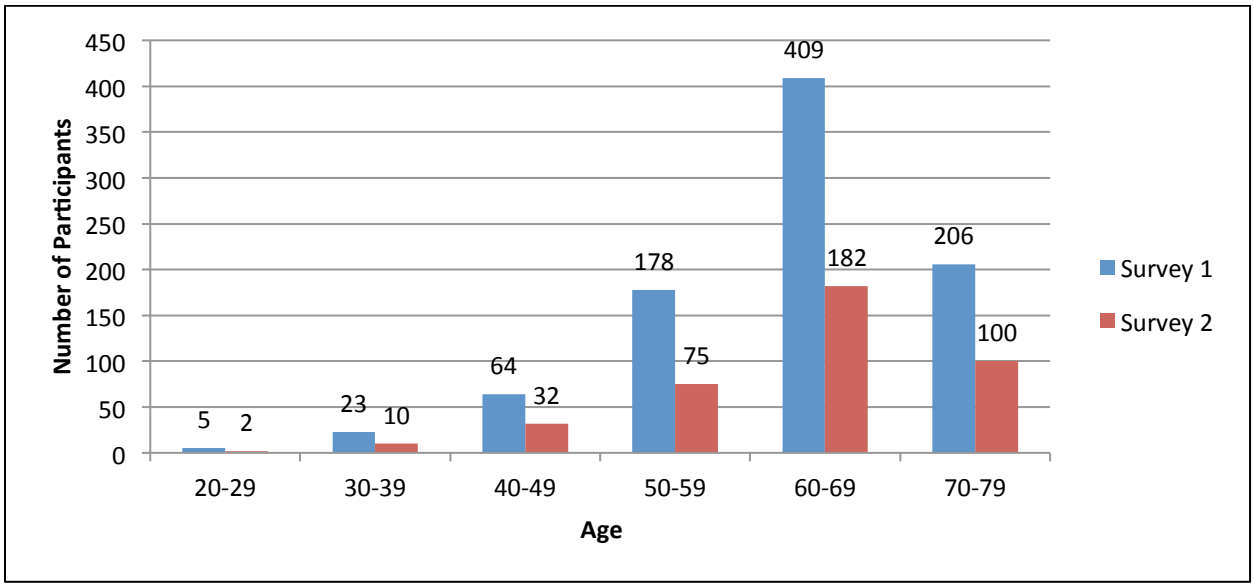

Fig. 6.5 Survey Participants' Age

Tests of the Hypotheses

Calculating Privacy Setting Usability and Information Practice Understanding

As mentioned previously, I used Facebook member's correct and incorrect responses from part 2(1) of the Facebook survey to determine both the "usability" variable for a privacy setting and the "understanding" variable for an information practice. Survey participants, of course, recorded their responses for this part using the free response fields—one for a URL, one for the user's explanation. I created a set of correct "benchmark answers" for each question. Due to the participant's free responses, however, scoring correct or incorrect answer could be subjective. Therefore, in order to determine members' ability to respond to each question, I firstly compared the member's responses to the benchmark answers. Secondly, I validated these results by having a second scorer evaluate participants' responses.

The comparison did validate that both scorer's results were accurate. The second scorer, of course, evaluated the questions for 10% of the participant population. For each question, the scorers did disagree over one or two participants' responses. However, 95.24% of the two scorers' results matched. In addition, I calculated the Cohen's Kappa statistic for inter-coder reliability using the two result sets. The statistic turned out to be 0.908 with a significance of $p < 0.000$. The scorer's results, therefore, should be highly reliable.

The results for questions relating to the usability of a privacy setting are as follows:

Privacy Setting Question	% Correct Participant Responses
Visibility of users' posts on user's wall/timeline	61.6%
Visibility of other users' posts on user's wall/timeline	73.2%
Tag suggestions	73.0%

Profile information (e.g. education, relationship status)	29.9%
Friends list	37.5%
Public search listing	44.5%
Information types friends can bring to their applications	69.7%
Instant Personalization	35.9%
Visibility of third-party social ads	11.5%

Table 6.1 Privacy Setting Usability Question Results

The results for questions relating to member's correct understanding of an information practice are as follows:

Information Practice Question	**% Correct Participant Responses**
Tagging Prevention	25.1%
Info Sharing with "Liked" Entities	76.9%
Visibility of Users' Posts on Others' Wall/Timeline	63.7%
"Social Plugin" User Monitoring	70.1%
Permanent Account Erasure	18.6%

Table 6.2 Information Practice Understanding Question Results

The actual content of participants' responses did provide insight in the results of hypotheses H_1, H_{2A} and H_{2B}. This content will be discusses following the tests of those hypotheses.

Calculating Member Privacy Conflicts

As mentioned previously, for each setting usability question, I calculated "privacy conflicts" by comparing the member's corresponding preferences and current settings selections. Unlike the usability questions, the preference and current selection questions used check boxes multiple-choice instead of free response to record users' answers. Therefore, instead of a subjective evaluation, I used two logical conditions based on these multiple-choice answers to calculate privacy conflicts. Firstly, for instance, a privacy conflict requires that the respondent indicates he or she "Did not prefer" or "Strongly did not prefer" the default privacy selection (the default for most Facebook privacy settings). Secondly, the respondent must have reported the current, corresponding setting selection as being the default selection. A respondent who meets both conditions for a privacy setting is likely sharing personal information he or she would prefer to keep private.

In determining privacy conflicts, I also took into account several complications in the survey. As mentioned in the "Methodology" chapter, I used the results from the second Facebook survey to determine conflicts for settings related to members' profile information and posts on their wall/timeline. Likewise, both the profile information setting and the setting governing the visibility of information to friends' applications, for instance, allow the user to select the visibility for each piece of information, such as the user's education, interests and photos. For these specific settings, therefore, I calculated a member's privacy conflict as the

proportion of the information with visibility settings at odds with the user's privacy preference. This allows the analysis to distinguish between participants that have privacy conflicts with the visibility for one or two pieces of information, and participants who have conflicts with all their profile information.

The results for privacy conflicts relating to privacy settings are as follows:

Privacy Setting	% of Concerned Participants with Privacy Conflicts
Visibility of users' posts on user's wall/timeline	10.9%
Visibility of other users' posts on user's wall/timeline	2.4%
Tag suggestions	56.4%
Profile information (e.g. education, relationship status)	14.3%
Friends list	15.8%
Public search listing	43.7%
Information types friends can bring to their applications	48.0%
Instant Personalization	36.8%
Third-party Social Ads	55.8%

Table 6.3 Privacy Conflict Results

Privacy Setting Hypothesis

This section, of course, tests hypothesis H_1: "The more usable a privacy setting is, the less likely it will be associated with privacy conflicts." As mentioned previously, the first Facebook survey did split the sample population so that half took the "usability" questions in part 2(1) and the other half contributed to the questions on "privacy conflicts." The second survey's population also contributed to the "privacy conflict" questions for "visibility of user's posts on his wall" and "profile information." Therefore, in order to use these split populations to test H_1, the "Privacy Setting" hypothesis, I performed a "split-halves" analysis. This type of analysis is fairly straightforward. To test hypothesis H_1, for example, this analysis will perform a qualitative comparison between each result for setting "usability" and the corresponding result for "privacy conflicts." The analysis may indicate, for instance, that the more usable a setting is, the fewer privacy conflicts users have relating to that setting. This finding would potentially indicate that the setting does help the user protect his information.

I also ran a "Multi-Dimensional Scale" on these variables to determine the goodness of fit for the results. The stress test came out to 0.266, indicating that the variables are a good fit and that the results should be reliable. The dissimilarity test came out to 0.233, indicating the results may have outliers. This analysis, therefore, performed the following comparison to test hypothesis H_1: "The more usable a privacy setting is, the less likely it will be associated with privacy conflicts."

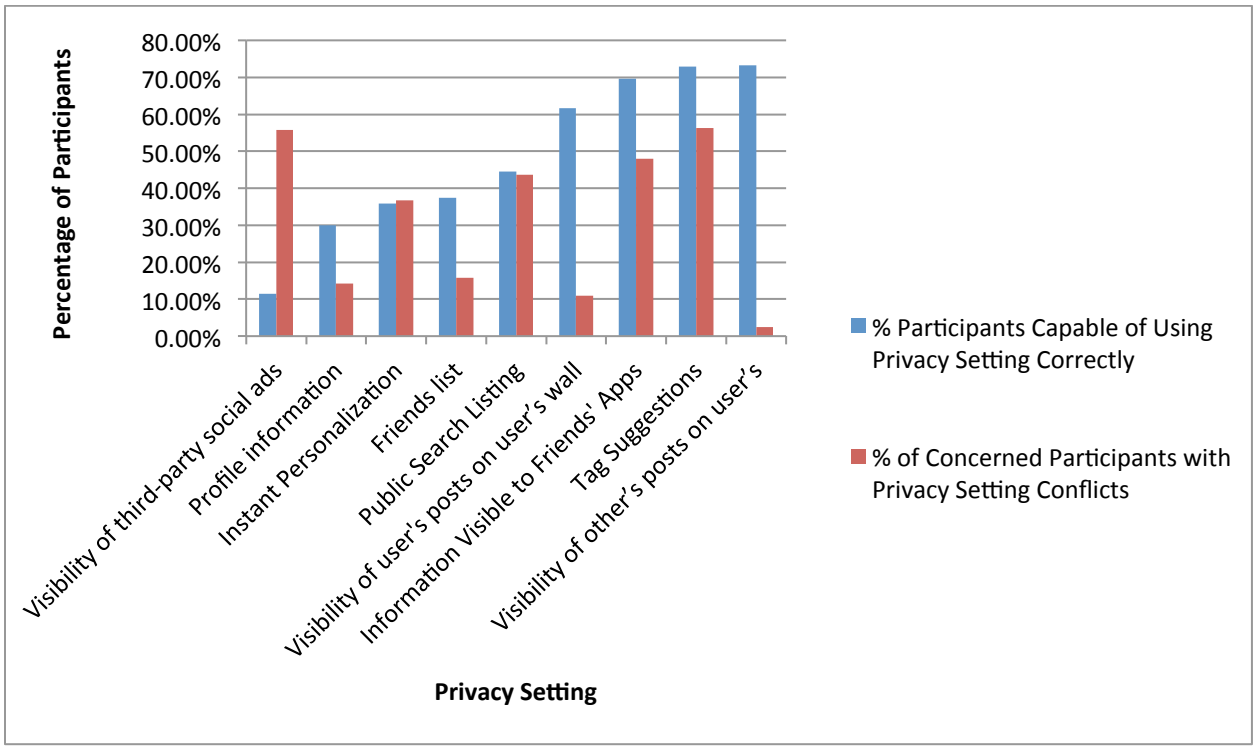

Fig. 6.6. Evidence for hypothesis H_1

The figure for hypothesis H_1 does indicate most of the settings (with the possible exception of "visibility of other's posts") have issues with usability or conflicts with user's preferences. Perhaps more importantly, however, the figure also appears to indicate that usability does not have an apparent relationship with the rate of privacy conflicts. The figure above, for instance, lists the privacy settings in order of increasing setting usability. Ideally, increasing numbers of Facebook members who can use the setting correctly should lead to decreasing numbers of user privacy conflicts. As the chart indicates, however, there does not appear to be a strong inverse relationship between the usability of a privacy setting and its associated conflict rate. To better examine the relationships in the data, I did calculate a trend line for privacy conflicts as a descriptive statistic. The trend line for the privacy conflict rates turn out to be almost flat, with a slope of -.0117. The slope's negative value does indicate some decrease in users with privacy conflicts, but it amounts to a drop of around 1.17% from one setting to the next.

The test of the hypothesis, therefore, does appears to indicate that the more usable a setting is, the more likely it is to be associated with privacy conflicts. As summarized previously, however, the goodness of fit indicates that these results accurately reflect trends in the data did not occur by chance. These results, therefore, provide weak support for hypothesis H_1.

"Inline" Setting Hypothesis

In addition, I also used the "split-halves" analysis to test the hypotheses related to "inline" privacy settings, H_{2A} and H_{2B}. In this test, however, instead of comparing the "usability"

variables with the "privacy conflict" variables, I will perform a separate, qualitative comparison for each set of variables between the groups allocated for "inline" privacy settings and menu-exclusive settings. For instance, to test hypothesis $H_{2A,}$ which relates to "privacy conflicts," I will compare the privacy conflict variables for the "'inline' settings" group with conflict variables for the "menu-exclusive setting" group. If, for instance, the conflict rates for the "'Inline' settings" group turned out to be lower overall than the rates for the "menu-exclusive" group, then this would support the hypothesis that "'Inline' settings are less likely to be associated with privacy conflicts than menu-exclusive settings."

I did consider using ANOVA, an "analysis of variance" approach, to test these hypotheses. However, separate populations from both the first and the second survey feed into the results for privacy conflicts. Moreover, the stress test for the "Multi-Dimensional Scale" in the hypothesis 1 test did come out to 0.266—indicating the variables are a good fit and I can trust any relationships found in the model did not occur by chance.

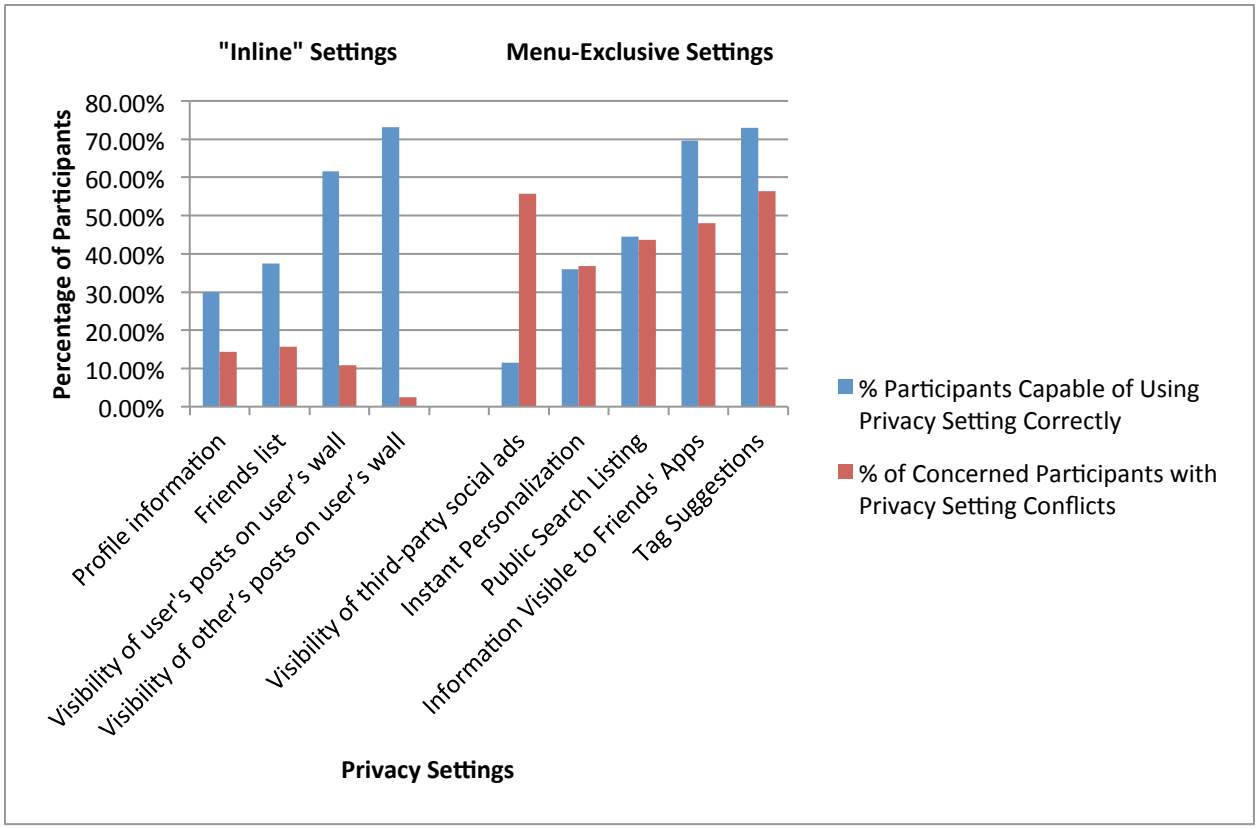

Fig. 6.7 Evidence for Hypotheses H_{2A} and H_{2B}

Examining the figure for hypotheses H_{2A} and H_{2B} does reveal several apparent relationships. Firstly, for instance, the privacy conflict rates for "inline" settings are substantially lower than the ones for menu-exclusive settings. The highest conflict rate for the "inline" settings group, for instance, is the "friends list" setting with a rate of 15.8%. The lowest conflict rate for menu-exclusive settings is the "Instant Personalization" setting, with a rate of 36.8%. The

privacy conflict rates for the "inline" settings group, therefore, are at a minimum 21.0% lower than the conflict rates for the menu-exclusive group. Therefore, I can reject the null hypothesis for H_{2A} and support the hypothesis that, "'Inline' settings are less likely to be associated with privacy conflicts than menu-exclusive settings."

Secondly, however, the "usability" rates for both groups do appear to be comparable. The usability rates for "inline" settings, for instance, range from 29.9% to 73.2%. The usability rates for menu-exclusive settings range from 11.5% to 73.0%, overlapping the rates for "inline" settings. To better examine the relationship between these two groups, I did calculate an average usability rate for both "inline" and menu-exclusive settings. The average "inline" setting usability turned out to be 50.55%. The average usability for menu-exclusive settings turned out to be 46.9%. "Inline" settings, therefore, do appear to be more usable than "menu-exclusive" settings, but the overall difference is small, less than 4%. These results, therefore, provide weak support for hypothesis H_{2B} that "'Inline' settings are less likely to be associated with privacy conflicts than menu-exclusive settings."

Privacy Setting Observations

The results for hypothesis 1, of course, do seem counter-intuitive. Privacy settings that are easier to use should be strongly associated with fewer conflicts with users' privacy preferences. The results, however, only reveal a weak relationship. Hypothesis H_{2A} does reveal the settings with the lowest conflict rates are actually the ones that use an "inline" privacy control. These include "profile information" with a rate of 14.3%, "Friends List" with a rate of 16.6%, "visibility of user's posts" with a rate of 29.8%, and "visibility of others' posts" with a conflict rate of 2.4%. Comparatively, menu-exclusive settings did have the highest usability rates, but they also had the most privacy conflicts. The "tag suggestions" setting, for instance, had a usability rate of 73.0%, but a conflict rate of 56.4%. The "Friends' Apps," "Public Search" and "Instant Personalization" settings had similar results. These findings do appear to indicate that users may be able to find these "menu" settings but, in practice, do not actually use them to protect information. However, to provide further insight into results for "inline" privacy settings, I examined the actual content of users' responses to the usability questions. The responses indicated that, although users may be capable of finding a setting on Facebook's "Privacy Settings" menu, many users actually mistake these "menu" settings as protecting information covered by "inline" controls.

The "profile information" setting, for instance, is actually an inline, pull-down menu located next to each piece of information on the user's profile page. In the survey, however, many respondents mistakenly indicated that the two privacy menu settings could protect their profile—"Default Privacy" and "Who can look you up?" This survey question had 271 incorrect responses. 74 users did pick "No Corresponding Setting." 71 users, however, picked "Who can look you up?" This setting is location under the "How You Connect" section in the privacy menu. According to the Facebook Help Center, it does not hide profile information, but it does control how a user can find another user's profile ("How do I control who can find me on Facebook"). Many users, of course, did not understand this distinction. One user, for instance, even indicated the setting and stated it controlled, "who can look *at* your profile?" Similarly, 62 users indicated the "Default Privacy" setting. Facebook placed this setting prominently at the top

of the privacy settings menu. Given the "default" term and the setting's visibility, a user could potentially believe the setting applied to all personal information on Facebook. However, the setting actually applies only to user's wall/timeline posts. Many users, of course, do not understand that nuance.

The "friends list" setting is also an inline, pull-down menu. Unlike "profile information," however, the majority of the incorrect responses had actually selected the "No Corresponding Setting" answer. A handful of survey respondents did indicate that the "Default Privacy" and "Who can look you up" settings can hide the user's friends list. In total, for instance, there were 240 incorrect responses. 30 users selected the "Who can look you up?" response and 18 selected "default privacy. However, 137 users picked the "No Corresponding Setting" option. Facebook's privacy setting menu does not explicitly mention "friends lists." Users, therefore, may have been less inclined to believe a setting on the privacy menu protect their list of friends. Moreover, Facebook has located the setting on the actual friends list page, separate from the privacy settings menu or the user's wall/timeline. Users therefore, may have had some difficulty in actually finding the setting. This could indicate that users expect to find privacy settings only in certain areas on Facebook, such as the privacy settings menu.

The setting for "visibility of user's posts on the user's wall" actually has both an "inline" and a "menu" privacy setting. The first, "inline" setting is a pull-down menu embedded in the post itself. The second is actually the "default privacy" setting, mentioned in the "profile information" discussion above. In comparison to the other two settings with "inline" controls, moreover, the privacy of "user's posts" clearly benefits from having a setting located in Facebook's privacy menu. The correct response rate for the setting's usability questions, for instance, was 31.7% higher than for "profile information." In addition, 48.5% of the correct responses chose the menu setting, "default privacy," as the answer. Many respondents, of course, still had difficulties identifying the correct privacy settings. The question had a total of 143 incorrect responses. 65 respondents still confused the "user's post" settings with the "Who can look you up?" setting that is also located in the privacy menu. 70 respondents selected "No Corresponding Setting." However, like "Friends List" the responses for the "user's posts" question appear to confirm that Facebook members are more capable of correctly using settings that appear where the members expect, such as in the "Privacy Settings" menu.

Unlike other "inline" settings, "visibility of others' posts" only has a non-interactive descript of the user's setting selection in the user post itself. The actual setting is located in the "How You Connect" section of the privacy menu.[d] Like, "visibility of others' posts," its usability rate also benefits for its location in the "Privacy Settings" menu. The setting's descriptor, moreover, is simply "Who can see what others post on your Profile?" This may help explain the setting's 73.2% usability score. The setting's usability question did have 100 incorrect responses. Similar the other setting, 39 of these were "No Corresponding Setting." 20 users also mistakenly indicated that the "Default Privacy" setting would protect others' posts on the user's wall.

Generally, settings located in the "Privacy Setting" menu, of course, had fewer incorrect responses. Survey participants did, however, still encounter difficulties in discerning which menu setting addresses which privacy issue. 213 respondents, for instance, did not correctly identify the setting to disable "public searches" via Google or Bing. Of those, 91 respondents

[d] Since the survey's completion, Facebook has moved this setting to the "Profile and Tagging" section.

answered with "Who can look you up?" Likewise, the "Friends' Apps" question had 112 incorrect responses. 30 of those respondents answered with the "Edit Apps You Use" setting, located in the "Apps, Games and Websites" section of Facebook's privacy menu. While this setting does allow a user to manage privacy for his or her application, it does not control what information other users' apps can access. The "tag suggestion" question, moreover, had 94 incorrect answers. 15 respondents answered with the "Tag Review" or "Profile Review" settings. All the usability questions, including these three, did have at least 40 to 70 incorrect responses with the "No Corresponding Setting" answer. Respondents may pick this option simply when they cannot find a viable answer. The "Instant Personalization" setting, however, had a total of 231 incorrect responses, with 171 of those being the "No Corresponding Section" answer. The usability question for this setting, however, spoke about sharing information with Bing or Rotten Tomatoes but did not mention "instant personalization" directly. Facebook privacy menu, however, titles the setting by that name. Several respondents, therefore, may have had difficulties understanding Facebook's "instant personalization" practice and its implications are for sharing personal data with other websites. Again, however, all the settings located in the "Privacy Setting" menu have high rates for usability.

Finally, the responses for "third-party social ads" also strongly indicate that the usability of a setting strongly depends on the setting's location on Facebook. This setting is actually not in the privacy menu but is actually in the "Account Settings" menu, under "Facebook Ads." The setting's usability question, moreover, had a total of 339 incorrect responses. Of these, 226 respondents chose the "No Corresponding Setting" answer. Respondents, therefore, appear to encounter difficult obstacles to finding and correctly using this setting. Contrary to the overall trend, moreover, the setting's conflict rate of 55.8% does seem to indicate that users' lack of ability to find and correctly use the setting is actually leading to issues with their current setting selections.

Privacy Setting	Incorrect Response Types	Number of Incorrect Responses	Total Number of Responses
Profile Information	**Total**	**271**	384
	No Corresponding Setting	74	
	Who can look you up?	62	
	Default Privacy	71	
Friends List	**Total**	**240**	382
	No Corresponding Setting	137	
	Who can look you up?	30	
	Default Privacy	18	
User's Posts Visibility	**Total**	**143**	370
	No Corresponding Setting	70	
	Who can look you up?	65	
Instant Personalization	**Total**	**231**	357
	No corresponding Setting	171	
	Edit Apps You Use	39	

Public Search Listing	**Total**	**213**	380
	No Corresponding Setting	77	
	Who can look you up?	91	
Info Visibility to Friends' Apps	**Total**	**112**	363
	No Corresponding Setting	66	
	Edit Apps You Use	30	
Tag Suggestions	**Total**	**94**	341
	No Corresponding Setting	62	
	Tag or Profile Review	15	
Others' Posts Visibility	**Total**	**100**	365
	No Corresponding Setting	39	
	Default Privacy	20	
	Who can post on your wall?	10	
User Info in Third-Party Social Ads	**Total**	**339**	381
	No Corresponding Setting	226	
	Social Ads setting (as opposed to Third-Party Ads setting)	34	
	Instant Personalization	19	
Info Sharing with "Liked" Entities	**Total**	290	389
	Tag and Profile Review	256	
Info Sharing with "Liked" Entities	**Total**	89	388
Visibility of Users' Posts on Others' Wall/Timeline	**Total**	141	388
	Who can see posts by Others on your Wall?	35	
"Social Plugin" User Monitoring	**Total**	115	387
	Instant Personalization	55	
Facebook Retains Info After Account Closure	**Total**	317	389
	No Corresponding Setting	104	
	Account deactivation	184	

Table 6.4 Common Incorrect Responses for Usability and Understanding Questions

Calculating Member Information Practice Preferences

The information practices, of course, do not have corresponding privacy settings. Therefore, I did not calculate the "privacy conflict" for each practice. However, the hypotheses for "information practices—H_{2A} through H_{2E} in the "Hypotheses" chapter—do compare users' understanding of an information practice with their preference for the practice. To prepare for the test of these hypotheses, therefore, I calculated users' preferences for each of the five practices. These calculations were relatively simple—a users who indicated in the survey that they "Did Not Prefer" or "Strongly Did Not prefer" an information practice counted as a participants who did not prefer that practice. Likewise, I also coded participants that answered a preference

question with “No preference,” “Prefer” or “Strongly Prefer” as accepting the corresponding information practice. The aggregate results are as follows:

Information Practice	% Participants Who Do Not Prefer Practice
Tagging Without Permission	52.81%
Info Sharing with “Liked” Entities	67.67%
Visibility of Users’ Posts on Others’ Wall/Timeline	58.43%
“Social Plugin” User Monitoring	70.08%
Facebook Retains Info After Account Closure	76.72%

Table 6.5 User Preferences for Information Practices Results

Information Practice Hypotheses

This section, therefore, tests the “information practice” hypotheses H_{3A}, H_{3B}, $H_{3C,}$ H_{3D} and H_{3E}. These tests compare users’ preferences with whether or not the user actually understands the information practice. Unlike, the “privacy setting” hypotheses, these tests do not need to use a split population to examine privacy conflicts. Therefore, I can directly correlate users who prefer or do not prefer an information practice with users who do or do not understand the same practice. In order to test hypotheses H_{3A}, H_{3B}, $H_{3C,}$ H_{3D} and H_{3E}, therefore, I used the “crosstabs” method. The method, for instance will examine the users who do not prefer an information practice and, for H_{3A}, H_{3B}, H_{3C} and $H_{3D,}$ compare the proportion of users who indicated “No Corresponding Setting” with the proportion who mistakenly indicated that a privacy setting would allow them to adjust or disable the practice. Hypothesis H_{2E}, of course, which deals with data retention after account closures, will compare proportions of users who did and did not identify that only “account deletion”—as opposed to “account deactivation”—would permanently delete their data. Finally, of course, each hypothesis test will also include a Fisher’s exact test of significance. The significance, of course, will indicate whether a result supporting the hypothesis is valid.

	"Information Practice" Hypotheses				
	Tagging Without Permission	Info Sharing with "Liked" Entities	Visibility of Users' Posts on Others' Wall	Monitoring via Social Plugins	Retention of Closed Account
Percentage of Participants with correct responses	25.1%	76.9%	63.7%	70.1%	18.6%
Percentage of Unconcerned Participants with Correct Responses	24.5%	80.7%	63.1%	67.1%	23.6%
Percentage of Concerned Participants with Correct Responses	25.4%	78.5%	64.1%	71.0%	16.7%
p value of significance	0.9029	0.3820	0.9125	0.4991	0.1428

Table 6.6 Test of "Information Practice" Hypotheses.

Unfortunately, the results for the tests of the "information practice" hypotheses did not turn out to be significant at the $p < 0.05$ level. The p value for "Retention of Closed Account" hypotheses H_{3E} did approach significance with a p value of 0.1458. Contrary to the hypothesis, however, nearly 6.9% more unconcerned participants had correct responses than participants who did not prefer Facebook retain closed account data. "Info Sharing with 'Liked' Entities" hypothesis H_{2B} also had more unconcerned than concerned participants with correct responses, though it had a p value of 0.3820. One possible explanation may actually be that, once a user understands an information practice, they become less concerned about the privacy implications and may come to have no preference or even prefer the practices. That being said, the low p values do not allow for statistically significant observations. The analysis therefore cannot support hypotheses H_{3A}, H_{3B}, $H_{3C,}$ H_{3D} and $H_{3E.}$

The content of users' incorrect responses, however, still does provide insight into users' understanding or misunderstanding of these information practices. As before, many users had difficulty discerning the scope of privacy settings seemingly related to the information practice. For instance, nearly 88% of incorrect responses for the "tagging prevention" questions cited the "Profile Review" and "Tag Review" settings located in the privacy menu. "Profile review" only prevents others' tagged content from appearing on the user's wall. "Tag review," of course, only governs whether others can tag the user's own content. These implications are confusing and appear to prevent users from understand the risk of someone else tagging them in a photo or post and circulating it. Likewise, over 50% of the incorrect responses for the "Retention of Closed Account" question indicated that "Account Deactivation" tool would permanently erase users' Facebook information. The "Account Deletion" tool does erase user information, but it is only accessible via the search bar. 33% of the incorrect responses, for instance, answered "No Corresponding Setting"—potentially indicating users could not find the deletion tool. Finally, the

incorrect responses for "info sharing with 'liked' entities," "visibility of users' posts on others' wall," and "monitoring via 'social plugins'" also indicate confusion with seemingly related settings.

Facebook Experience Hypotheses

This section, of course, will test hypotheses $H_{4A,}$ H_{4B} and H_{4C}. These hypotheses examine whether there is a relationship between the usability of a privacy settings and understand information practices with the users' experience on Facebook, including, including how many years they have had an account, how often they check for updates and how often they post. Since these tests did not involve current setting selections, they did not require split population. I drew the variables for user experience from part 4 of the original Facebook survey.

To represent setting usability and information practice understanding, I created an index using the results "understanding" and "usability" questions in part 2(1) of the survey. The Cronbach's alpha for this index came out to 0.587, indicating that the index is fairly reliable. Finally, to perform the comparison itself between these two sets of variables, I used Pearson correlations with two-tailed tests of significance. The results for these tests are as follows:

	Correlation with Usability and Understanding Index	Significance
Years on Facebook	0.112	0.054
Frequency Checking for Updates	-0.16	0.782
Frequency of Posts	0.035	0.547

Table 6.7 Test of "Facebook Experience" Hypotheses

The test resulted in two significant findings. Contrary to their respective hypotheses, the findings actually indicate that users who spent more years on Facebook are more capable of understanding information practices and using privacy settings correctly. The correlation between "Years on Facebook" and the "Overall" index resulted in a Pearson score of 0.112 and is approaching significance at the $p < 0.05$ level. Potentially, longer-term users may have more to experience privacy issues and familiarize themselves with related settings. A user embarrassed by friends' comments on his wall, for instance, may quickly learn the value of the "Who can see others' posts on your wall?" setting in the privacy menu.

Therefore, I can reject supports the null hypotheses for H_{4A} and support the hypotheses that, "the more years a user has had a Facebook account, the more likely the user will be capable of correctly using Facebook privacy settings or understanding information practices." The correlations for the remaining hypotheses, of course, were not statistically significant and therefore cannot reject the respective null hypotheses and support the hypotheses.

Hypotheses Comparing Timeline and Wall Formats

The last section will test hypotheses H_5. This hypothesis compares whether users with the "timeline" or "wall" format are more likely to be capable of correctly using privacy settings and understanding information practices. To represent users' "wall" or "timeline" format, I used the variable for the first question of Facebook. The "Usability" and "Understanding" index from the

"Facebook Experience" hypotheses again represented setting usability and information practice understanding. Comparing these variables did not require split population. To run the tests themselves, I performed an "Independent Samples T Test." For each of the indices, this method will compare the averages for users with "Timeline" format and users with the "Wall" format. The results are as follows:

Mean Difference	Levene's Test for Equality of Variance		T-Test for Equality of Means		
	F	Significance	T	Degrees of Freedom	Significance
-0.133	0.166	0.684	-0.435	296	0.664

Table 6.8: Test of "Timeline" and "Wall" Hypotheses H_{4A}, H_{4B} and $H_{4C.}$

The test did not result in a significant finding. The test had an F of 0.166 and a significance of $p > 0.05$, indicating equal variances. However, the test also had a T of -0.435 and 296 degrees of freedom, indicating the test was not significant at the $p < 0.05$ level with a p of 0.664. Moreover, the mean difference also turned out to be -0.133. This difference indicates users with the "Timeline" format are capable of correctly responding to 0.133 more "usability" or "understanding" questions than users with the "Wall" format. Given the "menu" index covers fourteen privacy settings and information practices, this difference appears negligible.These results cannot reject the null hypothesis for $H_{5.}$ Therefore, the results do not support the hypothesis that "Users that had the 'timeline' format are less likely than users with the 'wall' format to be capable of correctly using 'privacy menu settings.'"

Summary of Important Findings

My analysis of the survey results, therefore, resulted in the following significant findings: The test of H_1 provides weak support for the hypothesis that the more usable a privacy settings is, the less likely to be associated with privacy conflicts. Conversely, the test of H_{2A} provided strong support for the hypothesis that "inline" settings are less likely to be associated with privacy conflicts than menu-exclusive settings. The test of H_{2B} provided weak support for the hypothesis that users are less likely to be capable of correctly using "Inline" settings are more likely to be usable than menu-exclusive settings. Finally, the test for H_{4A} was statistically significant at the $p < 0.05$ level. Therefore, H_{4A} supported the hypothesis that the more years a user has had a Facebook account, the more likely the user will be capable of correctly using Facebook privacy settings or understanding information practices.

Chapter VI
Conclusion

Discussion

Perhaps the most startling conclusion, therefore, were the results for hypotheses for H_1 and H_{2A}. The test of the hypothesis for H_1 concluded that the usability does have an impact on the privacy conflict rate for a setting, but the impact is small. In fact, several individual settings that did achieve high usability rate, such as "tag suggestions" were also associated with a high rate of privacy conflicts. Conversely, other settings such as "profile information" scored poorly for usability but achieved the lowest rates for privacy conflicts in the study. On the other hand, however, as the hypothesis for H_{2A} indicated, the settings did fall into two distinct groups based on their conflict rates. The "inline" privacy settings, which cover profile information, friends lists and posts on the user's wall, consistently achieve conflict rates of less than 15.8%. The other, menu-exclusive settings, which cover third-party social ads, instant personalization, public search listings, friends' apps and tag suggestions, never achieved conflict rates of less than 37%. This distinction appears to be much stronger than the relationship suggested the results of the "usability" hypothesis. Therefore, usability was not the most important contributing factor to preventing privacy conflict. Instead, the settings that consistently had the lowest privacy conflict rates were those such as the "inline" settings, where the setting or the issue itself appears to create a "visceral" experience of privacy risk.

"Inline" Settings

The idea is that "visceral" privacy experiences, such as an explicit photo exposed on Facebook, strongly convey to users the importance of choosing protective setting selections. As Ryan Calo points out, "like language, experience has the capability of changing our mental models—that is, our understandings and assumptions about a given product, environment, or system" ("Against Notice Skepticism" 108). Likewise, as the analysis for "Facebook Experience" hypotheses indicated, users who have spent more years on Facebook—and therefore may have experienced more of these "visceral" incidents—are more capable of using Facebook settings correctly.

In particular, "inline" settings, therefore, appear to provide a more a more "visceral" experience because both the settings and the information they protect are more visible than for menu-oriented settings. Firstly, for instance, a user's profile information and his wall posts are perhaps the most visible pieces of information on Facebook. Secondly, the settings are located, "right next to the posts, photos and tags they affect" (Cox). These placements may serve as vivid reminders that the user has provided Facebook with personal information and could easily protect the privacy of that information.

The "profile information" setting, for instance, had the second-lowest usability score in the study. Nearly half of the incorrect responses for its usability question answered that the "Default Privacy" and the "Who can look up your profile?" would protect their profile

information. Respondents may have confused the "profile" term as applying to all Facebook. Likewise, the word "profile" would intuitively apply to "profile information." However, "profile information" appears to provide one of the more "visceral experiences" of Facebook. Pieces of profile information, including workplace and education, appear directly underneath the user's name in the user's "Timeline" or "wall." The "Profile information" setting selections, therefore, have garnered the third lowest conflict rate of 14.3%. The results for other "inline" settings also indicate that these "visceral" reminders lead to lower conflict rates. Facebook features the profile pictures for several of the user's friends on both "Timeline" and the wall. The setting, likewise, had conflict rate of 15.8%. Posts provide perhaps the most "visceral" experience on Facebook. Users interact with posts on their wall/timeline and they are aware of the visibility of others' posts on their newsfeed. Accordingly, the conflict rates came out to 10.4% for users' posts and only 2.4% for others'.

Other, Menu-Exclusive Settings

In contrast, exclusively menu-oriented settings such as "instant personalization" or "tag suggestions," appear to be less "visceral." Firstly, most of these settings are somewhat hidden in Facebook's "Privacy Settings" menu. A user concerned about this issue could easily intuit, for instance, that he or she could find the related setting in the "Privacy Settings" link that Facebook places at the top of each web page. However, the menu does not provide the same level of visibility as "inline" controls which, in turn, may provide users with less "visceral" incentive to change their privacy settings. Secondly, many of the specific privacy violations for these settings are often not public. A user, for instance, may mistakenly permit a friend's Facebook app to access the user's sensitive photos. Unlike the user's wall posts or profile information, however, there are no reminders that friends' apps can access the user's photos. The user, for instance, may only discover the violation if, by chance, the app publicizes the photo. This lack of publicity, therefore, may deprive users of the kind of "visceral" notice that helps drive them to protect profile information.

Therefore, the reason many of the settings for third-party sharing and similar issues achieved high usability rates but also high conflict rates appears to be that, although they appear simpler to use, they do not actually provide this "visceral" notice. These privacy settings for "Facial Recognition" and "Information Visible to Friends' Apps," for instance, both achieved usability rates of around 70%. "Tag suggestions," for instance, has a single privacy setting located in Facebook's privacy menu. The user can deactivate the suggestions fairly simply by switching the setting selection from "Friends" to "No one." However, as discussed, the menu setting does not provide a high level of visibility. Moreover, Facebook does not provide an indication or alert that it suggested a friend tag the user in a photo. As expected, therefore, over 56% of the users who did not prefer the "tag suggestions" practice had not deactivated the setting. Likewise, the setting for "Friends' Apps," is also relatively simple to use but faces similar issues. However, as discussed before, Facebook does not alert users or provide reminders when friends' apps access the user's information. Facebook members use checkboxes to select or deselect each type of information they want Friend's apps to see. The setting is intuitively located in Facebook's privacy menu, but this location also reduces the setting's level of

visibility. Accordingly, 48% of the users who did not want not want their information available to friends' apps share at least one piece of personal data.

Conversely, the "instant personalization" and "public search listing" issues do actually provide some form of privacy notice. However, while these notices do appear to contribute to lower conflict rates for either issue, they still appear to be less effective than the "inline" settings. Partners in the "instant personalization" program, such as Bing or Rotten Tomatoes, will display the user's Facebook name and often his or her profile photo when the user visits the website. Seeing his or her name listed next to a Facebook icon at the top of Bing could impel a user to investigate privacy settings. The name and photo alone, however, may not convey the risk of the site potentially sharing other information, such as sensitive photos. The location of the setting itself in the "Privacy Settings" menu, moreover, may still handicap its visibility. These factors explain why "instant personalization" still has a relatively high conflict rate of 36.8%. Similarly, "public search listing" makes the user's profile publicly available on search engines such as Google or Bing. However, only 47% of users search for themselves online (Madden). Users do not likely search for their information a regular basis. The "public search listing" setting, therefore, retained a relatively high conflict rate of 43.7%

Furthermore, in cases such as "instant personalization" or "information visible to friends' apps," Facebook may have implemented simple but less-effective setting in a rush to address privacy criticisms. In 2010, for instance, the EFF reported that, "Facebook has heard our complaints and has responded, giving back the ability to easily block… including web sites participating in Facebook's Instant Personalization program" (Bankston, "Facebook's New Privacy Improvements"). On the other side, however, ineffective settings, such as "third-party social ads," an ineffective setting may belie user consent for a particularly contentious privacy policy. As the setting's descriptor indicates, Facebook does not currently share user's name and profile picture with third-party social advertisers. However, Facebook has kept this setting so that, "if we allow this in the future, the setting you choose will determine how your information is used" ("Facebook Ads"). The usability score for this setting is 11.5%--the lowest in the study. Facebook located the setting under the "Account Settings" menu instead of "Privacy Settings." Over half of survey participants were unable to find it. Likewise, the setting does not appear to provide any "visceral" reminders for users to set the setting appropriately. Accordingly, over 55% of survey participants had given Facebook permission contrary to their preferences.

Implications

These results have several important implications for designing privacy settings on Facebook and other websites. Firstly, for instance, "Inline" settings do appear to be a privacy "best practice" potentially applicable to other websites. In a recent report on protecting consumer privacy, the FTC recommended that websites, "give consumers the ability to make decisions about their data at a relevant time and context" (*Protecting Consumer Privacy).* Twitter, for instance, currently does not provide an "inline" privacy setting for user "tweets." Many Twitter users, however, do publish explicit or sensitive information. An AT&T Research Lab report indicated, for instance, that "about a quarter of tweets do include information regarding when people are engaging in activities and where they are" (Humphreys, Gill, and Krishnamurthy 2). A user can use a checkbox in the "Setting" menu to limit the audience for tweets to pre-approved

followers. However, as the setting's descriptor states, "Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places" ("Account"). Twitter also does not provide an indication of a Tweet's "protected" or "public" status in the Tweet itself. Providing an "inline" setting in the posts themselves, therefore, would dramatically improve audience's understanding of the visibility for each tweet. This, in turn, could help inform their privacy decisions.

Secondly, these results overwhelming indicate that that Facebook needs to re-examine its approach to its "menu"-oriented privacy settings. One option might be, for instance, to visually organizing current setting selections and potential privacy risks on a "Privacy Dashboard." In 2009, for instance, Google released its own privacy dashboard. The dashboard lists by category, the quantities of data Google has collected about a user (Schonfeld). In addition, for each category, Google also provides a visually representative icon and a link to the related privacy settings. The idea, as Google states, is to, "greater transparency and control over your own data" (Whitten, Adan, and Mayer). In the past, Facebook did use a grid to convey users' current privacy selections for user posts and profile information (see fig. 7.1). A quick glance at the grid would reveal, for instance, the types of information the user shared with "everyone." Facebook replaced the grid with "inline" settings, which did locate the privacy controls next to the content itself. Facebook, however, could potentially use this grid format to represent other settings, such as "information available to friends' apps." This would provide the "visceral" experience of privacy risks that these settings currently appear to lack.

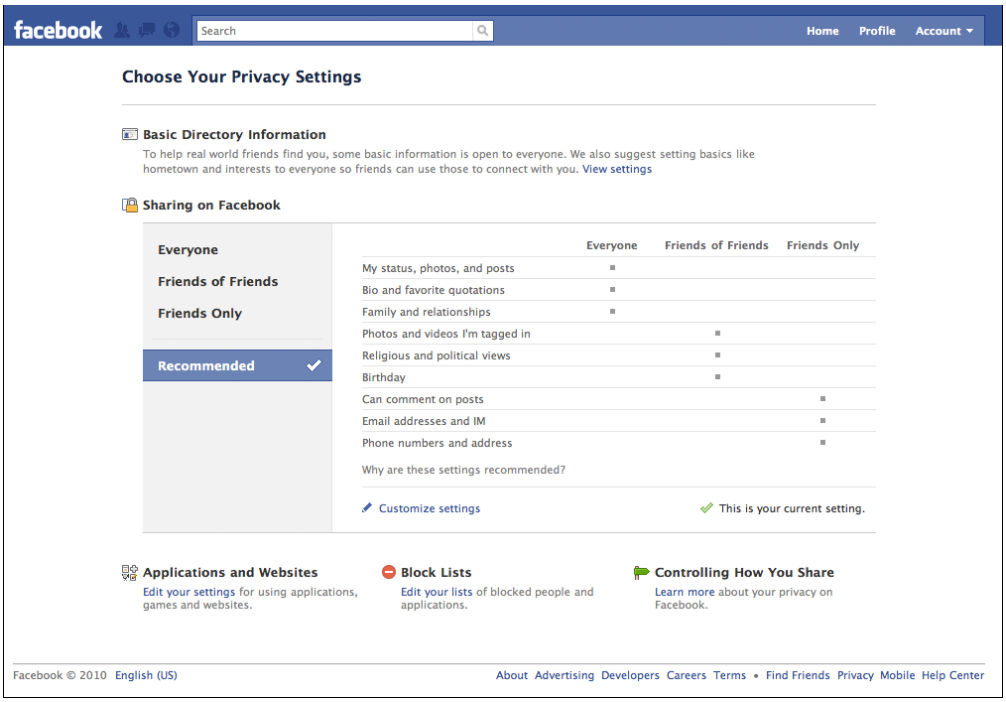

Fig. 7.1 Facebook Privacy Settings in 2010

Concluding Remarks

In conducting this study, I have formulated a unique, new methodology for calculating the "usability" of a privacy setting. Previous studies have examined privacy "conflict" by comparing user preferences and current setting selections, but many of these studies have not been able to address the source of these conflicts. A Columbia study examining privacy violations and Facebook wall posts concluded that, "additional research on the usability of privacy settings is necessary. Determining the root cause of violations is one possible follow-up" (Madejski, Johnson, and Bellovin 14). By calculating both the usability of privacy settings and user privacy conflicts, therefore, I have been able to provide new insight into how Facebook's settings help or hinder "notice-and-consent." The most surprising conclusion is that the usability of a privacy setting only has a weak connection to preventing conflicts between users' setting selections and their privacy preferences. Analyzing the results reveals, moreover, that settings located in menus are easy to find and use but lack visibility. Accordingly, I also concluded that Facebook's "inline" privacy settings were actually the most effective at preventing privacy conflict. "Inline" privacy settings consistently had conflict rates at least 20% lower than any other setting in the study. This conclusion implies that "inline" privacy settings would work as a "best practices for other sites such as Twitter. Conversely, this conclusion also implies that Facebook's exclusively menu-oriented settings, such as "information available to friends' apps" are the least effective at preventing privacy conflicts. These menu-oriented settings are often hidden in sub-menus and address behind-the-scenes data transactions, including sharing user information with apps, other websites, and even third-party advertisers. The study concludes, therefore, that Facebook has implemented several important settings, such as the "inline" controls, that do inform users' privacy decisions. For the remaining settings, however, especially those embedded in menu pages, Facebook need to find better ways to provide visibility into the setting selection and the protected information itself in order to provide "notice-and-consent."

This study examined the privacy settings that Facebook is currently using. Future work, however, may include calculating privacy conflicts involving setting designs other than "inline" controls or menu options. One good opportunity, for instance, would be to examine whether Google account owners' use of Google's privacy dashboard affects the privacy setting selections they make. Another option would be to examine whether Facebook members who regularly used the "profile preview" tool are more likely to make setting selections that match their preference. The Facebook survey for this study did include a usability question on "profile preview." The survey's split population, however, prevented any correlation with privacy conflicts rates. Research into these alternative setting designs, moreover, could provide insight into how Facebook can improve the visibility of its settings and "notice-and-consent" in general.

Works Cited

15 USC, Subchapter I, Sec. 6802(e)(3). <http://www.ftc.gov/privacy/glbact/glbsub1.htm#6802>.

“Account.” Twitter.com. Web. 25 Apr. 2012. <https://twitter.com/settings/account>.

Acquisti, Alessandro, and Jens Grossklags. "Privacy and Rationality in Individual Decision Making."*The Digital Technology Center*. University of Minnesota, 2004. Web. 29 Mar. 2011. <http://www.dtc.umn.edu/weis2004/acquisti.pdf>.

Anderson, Dave. "Google+ Learns From Facebook Privacy Mistakes." *International Business Times*. 12 Aug. 2012. Web. 26 Jan. 2012. <http://www.ibtimes.com/articles/197154/20110812/google-plus-learns-from-facebook-privacy-mistakes.htm>.

Angwin, Julia. "The Web's New Gold Mine: Your Secrets." *The Wall Street Journal*. 30 July 2010. Web. 25 Apr. 2012. <http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html>.

Bankston, Kevin. "Facebook's New Privacy Changes: The Good, The Bad, and The Ugly."*Deeplinks Blog*. Electronic Frontier Foundation, 2009. Web. 21 Feb. 2012. <https://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly>.

Bankston, Kevin. "Facebook's New Privacy Improvements Are a Positive Step, But There's Still More Work to Be Done." *Deeplinks Blog*. 26 May 2012. Web. 25 Apr. 2012.

<https://www.eff.org/deeplinks/2010/05/facebooks-new-privacy-improvements-are-positive>.

Beales, J. Howard, and Timothy J. Muris. "Choice or Consequences: Protecting Privacy in Commercial Information." *University of Chicago Law Review* 75.109 (2008): 109-35.

Bilton, Nick. "Price of Facebook Privacy? Start Clicking." *The New York Times*. The New York Times, 12 May 2010. Web. 21 Feb. 2012. <http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html>.

Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein. "Misplaced Confidences: Privacy and the Control Paradox." Proc. of Ninth Annual Workshop on the Economics of Information Security (WEIS), Harvard University, Cambridge, MA. 2010. Web. 21 Feb. 2012. <http://www.futureofprivacy.org/wp-content/uploads/2010/07/Misplaced-Confidences-acquisti-FPF.pdf>.

Taylor, Bret. "Applications Ask, You Receive: Simplified Permissions Launch." *The Facebook Blog*. Facebook.com, 30 June 2010. Web. 21 Feb. 2012. <https://blog.facebook.com/blog.php?post=403443752130>.

Calo, Ryan. "Against Notice Skepticism In Privacy (And Elsewhere)." *Notre Dame Law Review* 87 (2012): 101-44. *Social Science Research Network*. 21 Jan. 2012. Web. 26 Apr. 2012. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1790144>.

Calo, Ryan. "Facebook's New Privacy Tools As User Notice." *Stanford Center for Internet and Society*. Stanford University, 25 Feb. 2011. Web. 29 Mar. 2011. <http://cyberlaw.stanford.edu/node/6623>.

Cate, Fred H. "The Failure of Fair Information Practice." *Consumer Protection in the Age of the 'information Economy'* Ed. Jane K. Winn. Aldershot, Hants, England: Ashgate, 2006. 344-79. Print.

Conley, Chris. "The Social Network Is Stalking You." *Blog of Rights*. American Civil Liberties Union, 16 Nov. 2011. Web. 25 Apr. 2012. <http://www.aclu.org/blog/technology-and-liberty/social-network-stalking-you>.

Constine, Josh. "Facebook Launches New Application and Platform Privacy Dashboard."*Inside Facebook*. 6 Oct. 2010. Web. 21 Feb. 2012. <http://www.insidefacebook.com/2010/10/06/application-platform-privacy-dashboard/>.

Cox, Chris. "Making It Easier to Share With Who You Want." *The Facebook Blog*. Facebook.com, 23 Aug. 2011. Web. 21 Feb. 2012. <https://blog.facebook.com/blog.php?post=10150251867797131>.

"Data Use Policy." Facebook, 23 Sept. 2011. Web. 21 Feb. 2012. <https://www.facebook.com/full_data_use_policy>.

"Did the Internet Kill Privacy?" *CBSNews.com*. CBS News, 06 Feb. 2011. Web. 21 Feb. 2012. <http://www.cbsnews.com/2100-3445_162-7323148.html>.

Egelman, Serge, Janice Tsai, Lorrie Cranor, and Alessandro Acquisti. "Timing Is Everything? The Effects of Timing and Placement of Online Privacy Indicators." *SIGCHI Conference on Human Factors in Computing Systems*. 2009. Web. 26 Apr. 2012. <http://www.guanotronic.com/~serge/papers/chi09a.pdf>.

"EPIC Urges FTC Investigation into Facebook Timeline." Electronic Privacy Information Center, 28 Dec. 2011. Web. 25 Apr. 2012. <http://epic.org/2011/12/epic-urges-ftc-investigation-i.html>.

"Facebook Ads." Facebook.com. Web. 25 Apr. 2012. <https://www.facebook.com/settings?tab=ads>.

"Facebook Privacy." Electronic Privacy Information Center. Web. 21 Feb. 2012. <http://epic.org/privacy/facebook/>.

"Fact Sheet." *Newsroom*. Facebook.com. Web. 25 Apr. 2012. <http://newsroom.fb.com/content/default.aspx?NewsAreaId=22>.

Finin, Tim. "Project Gaydar and Privacy in Facebook and Other Online Social Networking Systems." *UMBC Ebiquity*. 20 Sept. 2009. Web. 25 Apr. 2012. <http://ebiquity.umbc.edu/blogger/2009/09/20/project-gaydar-and-privacy-in-facebook-and-other-online-social-networking-systems/>.

Gates, Guilbert. "Facebook Privacy: A Bewildering Tangle of Options." The New York Times, 12 May 2010. Web. 26 Apr. 2012. <http://www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html>.

Gross, Ralph, and Alessandro Acquisti. "Information Revelation and Privacy in Online Social Networks (The Facebook Case)." *ACM Workshop on Privacy in the Electronic Society (WPES)* (2005). Carnegie Mellon University. Web. 21 Feb. 2012. <http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf>,

Hastak, Manoj, and Mary J. Culnan. "Online Behavioral Advertising “Icon” Study." Future of Privacy Forum, 25 Jan. 2010. Web. 29 Mar. 2011. <http://futureofprivacy.org/final_report.pdf>.

He, Ray C. "New Privacy Controls for Your Applications." *The Facebook Blog*. Facebook, 17 Feb. 2010. Web. 21 Feb. 2012. <http://blog.facebook.com/blog.php?post=311056167130>.

"How do I control who can find me on Facebook with my contact info?" *Facebook Help Center*. Facebook.com. Web. 25 Apr. 2012. <https://www.facebook.com/help/?faq=131297846947406>.

" How do I control who can see what's on my profile (timeline)?" *Facebook Help Center*. Facebook.com. Web. 25 Apr. 2012. <http://www.facebook.com/help/?faq=167941163265974>.

Humphreys, Lee, Phillipa Gill, and Balachander Krishnamurthy. "How Much Is Too Much? Privacy Issues on Twitter." Proc. of Conference of International Communication Association, Singapore. 2010. Print.

"In Re Facebook and the Facial Identification of Users." Electronic Privacy Information Center. Web. 25 Apr. 2012. <http://epic.org/privacy/facebook/facebook_and_facial_recognitio.html>.

"Interactive Tools." *Data Use Policy*. Facebook.com. Web. 21 Feb. 2012. <https://www.facebook.com/about/privacy/tools>.

In the Matter of Facebook, Inc. Complaint, Request for Investigation, Injunction, and Other Relief Before the Federal Trade Commission. Electronic Privacy Information Center

(EPIC), 5 May 2010. Web. 21 Feb. 2012. <http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf>.

Jaycox, Mark M., and Rainey Reitman. "Facebook's (In)conspicuous Absence From the Do Not Track Discussions." *Deeplinks Blog*. Electronic Frontier Foundation, 15 Mar. 2012. Web. 25 Apr. 2012. <https://www.eff.org/deeplinks/2012/03/facebooks-inconspicuous-absence-do-not-track-discussions-when-individual>.

Jensen, Carlos, and Colin Potts. "Private Policies Examined: Fair Warning or Fair Game?"*SMARTech*. Georgia Tech Library and Information Center, 2003. Web. 28 Mar. 2011. <http://smartech.gatech.edu/handle/1853/3215>.

Kelley, Patrick G. "Conducting Usable Privacy & Security Studies with Amazon's Mechanical Turk." *CyLab Usable Privacy and Security Laboratory (CUPS)*. Carnegie Mellon University, July 2010. Web. 29 Mar. 2011. <http://cups.cs.cmu.edu/soups/2010/user_papers/Kelley_mTurk_USER2010.pdf>.

Kelly, Chris. "Improving Sharing Through Control, Simplicity and Connection." *The Facebook Blog*. Facebook, 1 July 2009. Web. 21 Feb. 2012. <http://blog.facebook.com/blog.php?post=101470352130>.

Lenhart, Amanda. *Cyberbullying*. Publication. Pew Internet & American Life Project, 27 June 2007. Web. 21 Feb. 2012. <http://www.pewinternet.org/Reports/2007/Cyberbullying.aspx>.

"Like." *Facebook Help Center*. Facebook.com. Web. 25 Apr. 2012. <http://www.facebook.com/help/like>.

Lipford, Heather R., Andrew Besmer, and Jason Watson. "Understanding Privacy Settings in Facebook with an Audience View." (2008). Web. 21 Feb. 2012. <http://static.usenix.org/event/upsec08/tech/full_papers/lipford/lipford.pdf>.

Madden, Mary. "Privacy Management on Social Media Sites." *Pew Research Center's Internet & American Life Project*. Pew Research Center, 24 Feb. 2012. Web. 25 Apr. 2012. <http://pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx>.

Madden, Mary, Susannah Fox, Aaron Smith, and Jessica Vitak. "Digital Footprints: Online Identity Management and Search in the Age of Transparenc." *Pew Internet and American Life Project*. Pew Research Center, 16 Dec. 2007. Web. 29 Mar. 2011. <http://www.pewinternet.org/Reports/2007/Digital-Footprints.aspx>.

Madejski, Michelle, Maritza Johnson, and Steven M. Bellovin. "The Failure of Online Social Network Privacy Settings." (2011). Web. 21 Feb. 2012. <https://mice.cs.columbia.edu/getTechreport.php?techreportID=1459>.

Mark MacCarthy. 2010. "New Directions in Privacy." *ExpressO.* <http://works.bepress.com/mark_maccarthy/2>.

McDonald, Aleecia, and Lorrie Cranor. "The Cost of Reading Privacy Policies." *I/S: A Journal of Law and Policy for the Information Society* 4.3 (2008): 540-63. Print.

McDonald, Aleecia, and Lorrie Cranor. "Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising." Proc. of Telecommunications Policy and Research Conference, George Mason University School of Law, Arlington, VA. 2010. Web. 21 Feb. 2012. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092>.

McDonald, Aleecia. "Footprints Near the Surf: Individual Privacy Decisions in Online Contexts." Diss. Carnegie Mellon University, 2010. *Research Showcase*. Carnegie Mellon University, 1 Dec. 2010. Web. 21 Feb. 2012. <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1008&context=dissertations>.

McDonald, Aleecia, Robert W. Reeder, Patrick G. Kelley, and Lorrie Cranor. "A Comparative Study of Online Privacy Policies and Formats." *Privacy Enhancing Techonologies Symposium* (2010). Web. 21 Feb. 2012. <http://lorrie.cranor.org/pubs/authors-version-PETS-formats.pdf>.

Mills, Elinor. "Facebook Finally Giving Users More Privacy Control." *CNET News*. CBS Interactive, 23 Aug. 2011. Web. 25 Apr. 2012. <http://news.cnet.com/8301-27080_3-20096136-245/facebook-finally-giving-users-more-privacy-control/>.

Mitchell, Justin. "Making Photo Tagging Easier." *The Facebook Blog*. Facebook.com, 30 June 2011. Web. 25 Apr. 2012. <http://blog.facebook.com/blog.php?post=467145887130>.

Nissenbaum, Helen Fay. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law, 2010. Print.

O'Neill, Nick. "INFOGRAPHIC: The History Of Facebook's Default Privacy Settings." *All Facebook*. 9 May 2010. Web. 21 Feb. 2012. <http://www.allfacebook.com/infographic-the-history-of-facebooks-default-privacy-settings-2010-05>.

Proferes, Nicholas. "Privacy: How Do We Define It, Assess It, And Then Seek to Protect It Online and Why?" *WRLC Digital Repository*, 24 Feb. 2010. Web. 29 Mar. 2011. <http://dspace.wrlc.org/dspace/handle/1961/6807>.

Schonfeld, Erick. "Google Gives You A Privacy Dashboard To Show Just How Much It Knows About you." *Tech Crunch*. 5 Nov. 2009. Web. 25 Apr. 2012. <http://techcrunch.com/2009/11/05/google-gives-you-a-privacy-dashboard-to-show-just-how-much-it-knows-about-you/>.

"Searching for People and Their Content." *Help Center*. Facebook. Web. 28 Feb. 2011. <http://www.facebook.com/help/?faq=16497>.

"Security Settings." Facebook.com. Web. 25 Apr. 2012. <https://www.facebook.com/settings?tab=security>.

Self-Regulatory Principles for Multi-Site Data. Rep. Digital Advertising Alliance (DAA), 2011. Web. 21 Feb. 2012. <http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf>, 2.

Taylor, Bret. "Applications Ask, You Receive: Simplified Permissions Launch." *The Facebook Blog*. Facebook.com, 30 June 2010. Web. 21 Feb. 2012. <https://blog.facebook.com/blog.php?post=403443752130>.

"Timeline." *Facebook.com*. Web. 26 Jan. 2012. <https://www.facebook.com/press/info.php?timeline>.

The Center for Information Policy Leadership. *Ten Steps to Develop a Multilayered Privacy Notice*. Rep. Hunton & Williams LLP, Mar. 2007. Web. 21 Feb. 2012. <http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Ten_Steps_whitepaper.pdf>.

Tsai, Janice, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study." *The 6th*

Workshop on the Economics of Information Security (WEIS). June 2007. Web. 26 Apr. 2012. <http://weis2007.econinfosec.org/papers/57.pdf>.

U.S. Department of Health and Human Services. *Notice of Privacy Practices for Protected Health Information.* 3 Dec. 2002. Web. 29 Mar. 2011. <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/notice.html>.

U.S. Department of Homeland Security. The Privacy Office. *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*. By Hugo Teufel. 29 Dec. 2008. Web. 26 Feb. 2011. <http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf>.

U.S. Federal Trade Commission. Bureau of Consumer Protection. Business Center. *In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act*. July 2002. Web. 29 Mar. 2011. <http://business.ftc.gov/documents/bus53-brief-financial-privacy-requirements-gramm-leach-bliley-act>.

U.S. Federal Trade Commission. Bureau of Consumer Protection. *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*. 2011. Web. 21 Feb. 2012. <http://ftc.gov/opa/2011/11/privacysettlement.shtm>.

U.S. Federal Trade Commission. *In the Matter of Facebook, Inc., a corporation. FTC File No. 092 3184*. 29 Nov. 2011. Web. 25 Apr. 2012. <http://ftc.gov/os/caselist/0923184/111129facebookagree.pdf>.

U.S. Federal Trade Commission. *Protecting Consumer Privacy in an Era of Rapid Change*. March 2012. Web. 25 April 2012. <http://ftc.gov/os/2012/03/120326privacyreport.pdf>.

Federal Trade Commission. *Privacy Online: Fair Information Practices in the Electronic Marketplace.* May 2000. Web. 29 Mar. 2011. <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>.

"What Information Does Facebook Get about Me When I Visit a Website with a Facebook Social Plug In?" *Facebook Help Center*. Facebook.com. Web. 25 Apr. 2012. <https://www.facebook.com/help/?faq=186325668085084>.

"What Is a Public Search Listing?" *Facebook Help Center*. Facebook.com. Web. 25 Apr. 2012. <http://www.facebook.com/help/?faq=124518907626945>.

Whitten, Alma, Yariv Adan, and Marissa Mayer. "Transparency, Choice and Control — Now Complete with a Dashboard!" *The Official Google Blog*. 5 Nov. 2009. Web. 01 Mar. 2011. <http://googleblog.blogspot.com/2009/11/transparency-choice-and-control-now.html>.

Zuckerberg, Mark. "An Open Letter from Facebook Founder Mark Zuckerberg." *The Facebook Blog*. Facebook, 1 Dec. 2009. Web. 01 Mar. 2011. <http://blog.facebook.com/blog.php?post=190423927130>.

Zuckerberg, Mark. "On Facebook, People Own and Control Their Information." *The Facebook Blog*. Facebook, 16 Feb. 2009. Web. 21 Feb. 2012. <http://blog.facebook.com/blog.php?post=54434097130>.

Zuckerberg, Mark. "Our Commitment to the Facebook Community." *The Facebook Blog*. Facebook, 29 Nov. 2011. Web. 21 Feb. 2012. <http://blog.facebook.com/blog.php?post=10150378701937131>.