An Empirical Study of the Level Of Agreement Between Social Media Users' Perceived and Actual Privacy Settings

By

Randolph G. Bias
Ramona Broussard
Samuel Burns

2015
UT CID Report #1512
Executive Summary

Motivated by popular press and research literature assertions about social media applications’ intentional or unintentional obfuscation of their privacy settings, we intended to investigate empirically the level of match between users’ actual and perceived privacy settings. In our study 1, a crowd-sourced survey asked 700 people about their use of five social media applications (Facebook, Twitter, Google+, Instagram, and Pinterest). Respondents claimed to affect their privacy settings on most of these “occasionally.”

Except for in Pinterest, the privacy settings for which people tended not to change, respondents were confident they knew where the privacy settings were (between 76% and 87% saying they were “confident” or “strongly confident”), and confident that their own settings matched their intentions (with between 68% and 81% saying they were “confident” or “strongly confident”).

In study 2 we interviewed 20 users of these social media applications, asking them the same questions about their perceived privacy settings, then asking them to go in to check to see if the settings matched their expectations. While, except in the case of Twitter, people expressed that that their actual settings matched well what they thought the settings to have been (with median scores ranging from 7 to 9 on a scale of 1 to 10 where 10 was “exactly matched my expectations”), 85% asserted that they did not know what one
or more of the privacy settings labels meant, and 75% of the interviewees, unbidden by the Investigator or the study instructions, either spontaneously made a change to their settings or expressed that they now intended to. Thus, while our users tended to express satisfaction with their privacy settings, once those settings were better understood our users tended to change them.

Future research will focus on the visualization of privacy settings, and on the usability of privacy settings in general.

**Introduction**

**Motivation/Problem Statement**

The headline of the New York Times article made it almost unnecessary to read the article: “Facebook Privacy: A Bewildering Tangle of Options” (New York Times, 2010). In the same issue another article warned: “But in recent months, Facebook has revised its privacy policy to require users to opt out if they wish to keep information private, making most of that information public by default. Some personal data is now being shared with third-party Web sites” (Bolton, 2010). Bolton continued: “As a result, the company has come under a blitz from privacy groups, government officials and its own users, who complain that the new policy is bewildering and the new opt-out settings too time-consuming to figure out and use.” And one more:

And still, some information will no longer remain private because Facebook has also added a feature, called community pages, which automatically links personal data, like hometown or university, to topic pages for that town or university. The only
way to disappear from those topic pages is to delete personal data from Facebook.

(Bolton, 2010)

Debatin et al. (2009) conducted a study in which they found “that most users do not realize that restricting access to their data does not sufficiently address the risks resulting from the amount, quality and persistence of data they provide” (no page number).

Nor is Facebook the only application or device for which it is an issue to accurately, quickly, confidently establish the settings you want.

Android briefly had a hidden feature called App Ops that let you tightly control each app’s permissions, but Google withdrew the feature three weeks after its launch late last year. Nonetheless, in Android versions 4.3 through 4.4.1, the basic App Ops settings can still be accessed via third-party controllers like App Opps 4.3/4.4 from Color Tiger. (McGarry, 2014)

A report titled “Toward better usability, security, and privacy of information technology” (2010) captured the situation well: “More usable security can help avoid the inadvertent (or even deliberate) undermining of security by users. Indeed, without sufficient usability to accomplish tasks efficiently and with less effort, users will often tend to bypass security features” (p. vii). The same report offered:

Moreover, security and privacy technologies originally were developed in a context in which system administrators had primary responsibility for security and privacy protections and in which the users tended to be sophisticated. Today, the user base is much wider—including the vast
majority of employees in many organizations and a large fraction of households—but the basic models for security and privacy are essentially unchanged. Security features can be clumsy and awkward to use and can present significant obstacles to getting work done. As a result, cybersecurity measures are all too often disabled or bypassed by the users they are intended to protect. (p. 4)

Concerns about identity theft (e.g., Madden, Lenhart, Cortesi, & Gasser, 2013) drove McGlone et al. (2015) to the “development of an instrument for measuring consumers’ ‘baseline’ understanding of the issue and the impact these [educational] materials may have on their subsequent beliefs, attitudes, and behaviors” (p. 1). With this study we intended to add empirical data regarding the match, or mismatch, between people’s perceived privacy settings, in social media applications, and their actual settings.

Some existing literature has begun to address the problems of these mismatches. In their paper on privacy and social media, Liu et al. (2011) write, “Just a few of the reasons for privacy violations include poor human–computer interaction mechanisms, the static nature of privacy settings, and the significant amount of work forced on the user to maintain the privacy of their content.” Some other work has addressed human-computer interaction issues and the amount of work required to maintain.

Firstly, some research has investigated the issue of human-computer interaction or poor usability for privacy features in social media. As Madejski et al. put it, “Access control policies are notoriously difficult to configure correctly” (2011). In a 2009 project, Lipford
et al. suggest that helping users see how others will see their pages will provide help for some of the confusion that underlies people’s mismatched perceptions.

Other researchers have investigated the second issue from the analysis of Liu et al. (2011): the issue of amount of work maintaining privacy on social media requires. These researchers investigate this to address the degree to which mismatches in intentions and actual settings indicates that people are disinterested in privacy. boyd (2008) and Hargittai (2010) find that users are concerned about their privacy and are often discontented with what they find out about their privacy on social media. Notably, Hargittai (2010) found a positive relationship between likelihood to have adjusted privacy and frequency of use.

So while people who frequently use social media are likely to also more frequently adjust settings and work on maintaining privacy, issues of usability and privacy discontent persist.

**Goals**

The Center for Identity website lists among its goals “Educating students, government, businesses, and the public concerning threats, best practices, and solutions for identity management, security, and privacy for individuals and organizations” (Center for Identity, 2015). This study was intended to address this explicitly. All the software applications and best practices are of no value if actual users are not able to discern what their privacy settings are, and to set them to match their personal intentions.
Are we sharing what we think we're sharing, online? Are we providing applications and third-parties more freedom to use and share our pictures and other personal information beyond what we think we are? Our goal in this study was to empirically determine if social media application users' privacy settings, on their own devices, are what they think they are. If we found that there is a mismatch between people's perceived and actual privacy settings, it would, we hoped, empirically motivate more attention paid to the design of clear, user-friendly user interfaces (UIs) to enable people to easily and accurately establish the settings they wish to have.

Objectives

Our objectives were to:

- Collect baseline, 2015 data on the accuracy of people's perception of their privacy settings and their confidence in that perception.

- Extend the work of the McGlone et al. (2015) Identity Literacy Scale to include consideration of users’ confidence in their own privacy settings.

- Empirically motivate attention to, and demonstrate the robust return-on-investment (ROI) in, a user-centered design approach to privacy setting UIs

Research Questions

- Do consumers have an accurate perception of their own privacy settings in their social media applications?

- Might the emerging Identity Literacy Scale, as developed by McGlone et al. (2015), be expanded to include user’s perceptions of their privacy settings?
Keywords

Usability; User-centered design; Privacy settings; Identity Literacy; Mismatch between perceived and actual privacy settings

Method

Our study design included two stages: 1) an online survey in which 700 people answered a questionnaire about their perceptions of privacy on social media, for which we recruited participants via the Amazon Turk service, and 2) exploratory in-person interviews with 20 people about their experiences with privacy on social media for which we recruited adults from inside and outside the University via convenience and snowball sampling.

Study 1

Study 1 was a crowdsourced study (see Liu, Bias, Lease, and Kuipers, 2012), where remote, “faceless,” unidentified workers carried out a brief task (completion of a survey) and were paid $1.00. Amazon Turk also charges 40% for batches of more than 20, so each participant effectively cost $1.40.

In the McGlone et al. (2015) crowdsourced study, “respondents were recruited through Mechanical Turk (www.mturk.com), an online platform operated by Amazon.com. MTurk is a crowdsourcing labor market in which employers (‘requesters’) post advertisements for human intelligence tasks (‘HITs’) and employees (‘workers’) perform those tasks for compensation. Participants were paid $1.00 for completing the scale” (p. 1).
As in that study, we imposed the following stricture on our crowdsourced test participants, to ensure maximal comparability between the two studies: “...workers were required to have completed at least 100 previous HITs in MTurk and have 95% or higher approval ratings from prior requesters.”

As in the McGlone et al. (2015) study, we administered an online survey using Qualtrics software (version 18.856s), for which UT-Austin holds a license. Respondents gained access to the survey in Qualtrics via an advertisement posted in MTurk recruiting volunteers for a “study of beliefs and attitudes about identity theft and of individual's understanding of their own privacy settings” (McGlone et al., 2015, p. 1). We provided an informed consent form, an overview of the study, and specific instructions to be read by the participant (Appendix A). After completing the survey (Appendix B) the participant was provided a passcode to allow him/her to claim payment in MTurk. Qualtrics has built-in features to ensure that online users do not take the survey more than once.

The survey itself took approximately 8 minutes to complete. We first included five demographic questions (gender, country of residence, age, income, and technological knowledge).

The survey entailed two of the four sections from the McGlone et al. (2015) scale, plus a new section on perceived level, and perceived level of confidence in, one’s own privacy settings for certain social media applications. That is, first participants saw and responded to the questions from the McGlone et al. (2015) study in the PII (Personally Identifiable
Information) Awareness and Prevention Awareness sections of their survey. This from the McGlone et al. (2015) paper:

PII Awareness Factors. Respondents sensitivity ratings of what constitutes PII clustered into 5 distinct factors: “Stable Individual Characteristics” (9 items, explaining 23% of rating variance), “Contact Information” (5 items, 12.2%), “Credentials” (5 items, 11.5%), “Behavioral Data” (5 items, 11.3%), and “Common Authentifiers” (2 items, 6.1%). Scale reliabilities ranged from $\alpha = .93$ to $.75$. (p. 2)

Because it includes the question about “Carefully Read Privacy Policies,” we also included the McGlone et al. (2015) “Prevention Awareness Factors”:

Prevention Awareness Factors. Three factors emerged from effectiveness ratings of the prevention strategies: ‘Data Elimination Strategies’ (6 items), ‘Disclosure Avoidance Strategies’ (6 items), and ‘Data Protection Strategies’ (6 items). Scale reliabilities ranged from $\alpha = .92$ to $.68$. (McGlone et al., 2015, p. 2)

Then, subjects were asked four questions about their confidence in their understanding of their privacy settings, and the protection of their personal information, for two of the following five applications/software services that they purported to use:

- Facebook
- Google services
- Twitter
- Pinterest
- Instagram
Social Media Selection

We selected these five of the most popular social media applications based on two criteria. Firstly we wanted to provide questions for participants about some of the most popular social media applications. To that end we used an update from a Pew Internet survey (2014) and a report on social networking sites from Alexa.com (2015). Secondly, to further narrow the number of applications we were asking participants about, we chose to select from the range of social media those that specifically offer users places to connect with friends and post asynchronous personal updates. We considered text or images to be personal updates, whether original content or reposted from elsewhere. To limit our scope, we did not consider video social media for this study (such as YouTube or Vine), nor did we consider social media explicitly designed for synchronous “chat” or messaging (such as Slack or Snapchat).

The five applications we chose to consider thus are reasonably popular places for users to post text and images for the purpose of networking: Facebook, Google Plus, Twitter, Pinterest, and Instagram. Our selections have a range of kinds of privacy that they offer, providing participants in our interviews with plenty of opportunity to compare complexity and modes of use when discussing privacy. The five selections have enough similarities to be comparable, but also offer some telling differences that enabled participants to discuss privacy concerns across contexts.

Study 2
In Study 2 we administered the same survey in person to 20 people locally in Austin, half (10) from the UT campus (students, faculty, staff), and 10 Austinites not associated with UT. (This, to get a broad spectrum, we hoped, of technological literacy.) After completion of the survey, each subject underwent an ethnographic interview (see Spradley, 1979) by a researcher, to better understand the subject’s perception of his/her privacy settings on various social networking apps and services that the subject had claimed to use. As in the crowdsourced study, we chose two of the applications the test participant purported to use with some frequency. Our goals in selecting two applications, when the test participant listed more than two, were to a) limit the length of the interview, and b) to get as much breadth of coverage as possible. That is, if some test participant expressed use of an application for which we had relatively little feedback, we asked about that one. Then, the researcher worked with the subject to go into the subject’s settings, to see how closely the actual settings match his/her perceived settings.

After each participant completed the online survey, the moderator asked him or her to log into the two accounts selected for review. The moderator then walked the participant through his/her privacy settings on each platform. The moderator sat across from the participant while the participant used a computer provided with the browser in “incognito” mode (not saving passwords or cookies). The moderator asked the participant to describe his or her settings out loud without revealing anything identifying or anything they “just didn’t feel comfortable with revealing.” In the second participant session, the participant asked if she could change her settings during the session. Our protocol included a question about whether participants wanted to change their settings, but we had not anticipated
they would want to do so during the session. We decided to allow it, and following that session we decided that if participants asked to do so (or did so without asking the moderator) we allowed it and marked that fact it in our notes. So we did not suggest they change anything or say anything about changes during the review unless they explicitly asked us (and we noted when they did not ask but said out loud that they changed something).

How many settings participants needed to review varied based on which platform was being considered and on what the particular settings were. For example, on Facebook, we had them go to settings, then check more than 20 individual settings in five different sections such as “who can see my stuff” and “blocked” user lists. For Facebook, if they allowed only “friends” to follow them, there were no further settings in that section, whereas if they allowed more freedom there then there were additional settings. On Instagram, in contrast, there was only one setting for privacy (on or off). We did not review security settings (e.g., passwords). If participants asked to change something in their settings, we allowed them to do so and made a note of it.

Once they completed the walkthrough of their settings, we asked them a series of interview questions about their settings and their past experiences with privacy on the two platforms they reviewed settings on. This allowed participants to compare and contrast the two platforms they answered about. Interview questions are included below in Appendix D.

Note, this affords us an empirical measure of any potential mismatch between the perceived and actual settings, plus the potential for subsequent correlations between the
Identity Literacy Scaling data and the strength of the match between a subject’s actual and perceived privacy settings. Also, combined with the results of Study 1, we have a measure of how appropriately-, or under-, or over-confident people are, in their estimation of their understanding of their own settings.

Results

Study 1

Of 700 paid respondents who were deemed to be real humans and not software bots or other agents, 68% were from the United States, 29% were from India, with no other country having more than two respondents. The median age range of our respondents was 25-34 years, and their median household income was $30,000 - $39,999.

The following table reflects the social media platforms used by our respondents. (Note, this was a multi-select question – respondents could claim to use any of these applications.)

Which of the following social media platforms do you have an active account on? (Select as many as you like, we’ll assign you questions about only 2 of them).
Which of the following social media platforms do you have an active account on? (Select as many as you like, we'll assign you questions about only 2 of them).

<table>
<thead>
<tr>
<th>#</th>
<th>Answer</th>
<th>Response</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Facebook</td>
<td>663</td>
<td>92%</td>
</tr>
<tr>
<td>2</td>
<td>Twitter</td>
<td>389</td>
<td>54%</td>
</tr>
<tr>
<td>3</td>
<td>Google+</td>
<td>257</td>
<td>36%</td>
</tr>
<tr>
<td>4</td>
<td>Instagram</td>
<td>204</td>
<td>28%</td>
</tr>
<tr>
<td>5</td>
<td>Pinterest</td>
<td>164</td>
<td>23%</td>
</tr>
</tbody>
</table>

• Table 1: Particular social media applications used.

Table 2 reflects frequency of usage of each of the studied applications.

<table>
<thead>
<tr>
<th>Frequency of Use</th>
<th>Facebook (N=558)</th>
<th>Twitter (N=289)</th>
<th>Google+ (N=176)</th>
<th>Instagram (N=124)</th>
<th>Pinterest (N=94)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than twice a month</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>2-3 times a month</td>
<td>6%</td>
<td>19%</td>
<td>31%</td>
<td>16%</td>
<td>33%</td>
</tr>
<tr>
<td>Once a week</td>
<td>7%</td>
<td>14%</td>
<td>13%</td>
<td>15%</td>
<td>19%</td>
</tr>
<tr>
<td>2-3 times a week</td>
<td>15%</td>
<td>32%</td>
<td>32%</td>
<td>26%</td>
<td>35%</td>
</tr>
<tr>
<td>Daily or more</td>
<td>71%</td>
<td>35%</td>
<td>24%</td>
<td>44%</td>
<td>13%</td>
</tr>
</tbody>
</table>

• Table 2: Frequency of usage

Next we were interested in how often participants change their account settings across the five applications.

<table>
<thead>
<tr>
<th>Frequency of Acct. Settings Change</th>
<th>Facebook (N=558)</th>
<th>Twitter (N=289)</th>
<th>Google+ (N=176)</th>
<th>Instagram (N=124)</th>
<th>Pinterest (N=94)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all</td>
<td>19%</td>
<td>47%</td>
<td>33%</td>
<td>45%</td>
<td>74%</td>
</tr>
<tr>
<td>Occasionally</td>
<td>70%</td>
<td>49%</td>
<td>62%</td>
<td>51%</td>
<td>23%</td>
</tr>
<tr>
<td>Frequently</td>
<td>11%</td>
<td>4%</td>
<td>5%</td>
<td>4%</td>
<td>2%</td>
</tr>
</tbody>
</table>
• Table 3: Frequency of changing account settings

We wanted to know with whom people tend to share their content, on the various platforms.

<table>
<thead>
<tr>
<th>With whom do you share content?</th>
<th>Facebook (N=558)</th>
<th>Twitter (N=289)</th>
<th>Google+ (N=176)</th>
<th>Instagram (N=124)</th>
<th>Pintrest (N=94)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyone</td>
<td>18%</td>
<td>54%</td>
<td>23%</td>
<td>49%</td>
<td>55%</td>
</tr>
<tr>
<td>Just my friends</td>
<td>59%</td>
<td>31%</td>
<td>52%</td>
<td>42%</td>
<td>22%</td>
</tr>
<tr>
<td>Friends and their friends</td>
<td>19%</td>
<td>10%</td>
<td>12%</td>
<td>5%</td>
<td>9%</td>
</tr>
<tr>
<td>No one</td>
<td>3%</td>
<td>6%</td>
<td>11%</td>
<td>4%</td>
<td>13%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
<td>0%</td>
<td>2%</td>
<td>0%</td>
<td>1%</td>
</tr>
</tbody>
</table>

• Table 4: With whom do people share content, on various platforms

The next two questions addressed perceived confidence in knowing where to find an application’s privacy settings and, the crux of this study, how confident the respondents were that their settings reflected their intentions.

<table>
<thead>
<tr>
<th>Confidence in finding privacy settings</th>
<th>Facebook (N=558)</th>
<th>Twitter (N=289)</th>
<th>Google+ (N=176)</th>
<th>Instagram (N=124)</th>
<th>Pintrest (N=94)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly confident</td>
<td>39%</td>
<td>25%</td>
<td>27%</td>
<td>26%</td>
<td>17%</td>
</tr>
<tr>
<td>Confident</td>
<td>48%</td>
<td>45%</td>
<td>52%</td>
<td>50%</td>
<td>37%</td>
</tr>
<tr>
<td>Neither confident nor unconfident</td>
<td>5%</td>
<td>15%</td>
<td>9%</td>
<td>11%</td>
<td>15%</td>
</tr>
<tr>
<td>Only slightly confident</td>
<td>7%</td>
<td>10%</td>
<td>10%</td>
<td>10%</td>
<td>22%</td>
</tr>
<tr>
<td>Not at all confident</td>
<td>1%</td>
<td>4%</td>
<td>2%</td>
<td>2%</td>
<td>9%</td>
</tr>
</tbody>
</table>
• Table 5: Confidence in being able to find privacy settings

We note here that in Pinterest, which we learned earlier was the application with the least frequent changes, only 54% of the respondents were “confident” or “strongly confident” they knew where to locate the privacy settings, whereas the other four applications yielded between 70 and 87% responses in the combined “confident” and “strongly confident” categories.

<table>
<thead>
<tr>
<th>Confidence privacy settings are as you want them</th>
<th>Facebook (N=558)</th>
<th>Twitter (N=289)</th>
<th>Google+ (N=176)</th>
<th>Instagram (N=124)</th>
<th>Pintrest (N=94)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly confident</td>
<td>25%</td>
<td>22%</td>
<td>22%</td>
<td>22%</td>
<td>15%</td>
</tr>
<tr>
<td>Confident</td>
<td>49%</td>
<td>46%</td>
<td>59%</td>
<td>56%</td>
<td>29%</td>
</tr>
<tr>
<td>Neither confident nor unconfident</td>
<td>11%</td>
<td>16%</td>
<td>11%</td>
<td>11%</td>
<td>28%</td>
</tr>
<tr>
<td>Only slightly confident</td>
<td>13%</td>
<td>13%</td>
<td>5%</td>
<td>10%</td>
<td>17%</td>
</tr>
<tr>
<td>Not at all confident</td>
<td>3%</td>
<td>3%</td>
<td>3%</td>
<td>1%</td>
<td>12%</td>
</tr>
</tbody>
</table>

• Table 6: Confidence that the privacy settings are as intended

Here is a potentially interesting finding. The five applications ranged from 44% (Pinterest) to 81% (Google+) in the percentage of respondents who were confident the settings were as the respondent intended them to be. But while Facebook yielded the highest percentage (87%, with Google+ being in second place with 79%) of respondents who were confident they knew where to locate the privacy settings, Facebook yielded only the third highest confidence (74%, to the Google+ 81%) that the settings were as intended.
Next we asked two questions, about each of the applications of interest, about sharing of information incorrectly, or against one’s will.

<table>
<thead>
<tr>
<th>Has anyone else ever shared something about you you with they hadn’t on this app</th>
<th>Facebook (N=558)</th>
<th>Twitter (N=289)</th>
<th>Google+ (N=176)</th>
<th>Instagram (N=124)</th>
<th>Pintrest (N=94)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>36%</td>
<td>11%</td>
<td>9%</td>
<td>13%</td>
<td>2%</td>
</tr>
<tr>
<td>Not sure</td>
<td>19%</td>
<td>19%</td>
<td>23%</td>
<td>15%</td>
<td>11%</td>
</tr>
<tr>
<td>No</td>
<td>45%</td>
<td>70%</td>
<td>68%</td>
<td>72%</td>
<td>87%</td>
</tr>
<tr>
<td>Other</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

- **Table 7**: Others’ having shared participant information that the participant wished they had not

<table>
<thead>
<tr>
<th>Have you ever shared content you wish you hadn’t</th>
<th>Facebook (N=558)</th>
<th>Twitter (N=289)</th>
<th>Google+ (N=176)</th>
<th>Instagram (N=124)</th>
<th>Pintrest (N=94)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>23%</td>
<td>9%</td>
<td>13%</td>
<td>6%</td>
<td>4%</td>
</tr>
<tr>
<td>No</td>
<td>77%</td>
<td>90%</td>
<td>86%</td>
<td>94%</td>
<td>96%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

- **Table 8**: Participants having shared information they wish they hadn’t

Perhaps the most interesting finding here is not that Facebook has led the highest incidence of undesired sharing, but rather that each of the applications has led to some.

**Study 2**

We first measured participants’ expectations and their perception of whether those expectations matched reality (from the walkthrough). For four of five platforms, after reviewing their privacy settings, people estimated that their settings were close to what
they had expected (they rated them between 7 and 9 on a 10-point scale). For one platform, Twitter, most people estimated that the settings did not match what they had expected – an average of 3 on the 10-point scale.

Expectations

Our participants expressed that they had a low degree of expectations for privacy on any of the 5 platforms. With the exception of Twitter, participants indicated that settings matched their expectations more than they did not match. Participant-rated averages on a scale of 1-10, 10 being “exactly matched my expectations” were as follows:

- Facebook: 8.2
- Google+: 7
- Twitter: 3
- Pinterest: 8
- Instagram: 9

The following comment is one example of the relatively low expectations for privacy that our participants described ("P" = Participant; “I” = Investigator):

P: “Well. I assumed I wouldn’t like the way any of the settings were. So I would say that was a very accurate idea of what happened. I feel like Facebook is constantly
trying to open up privacy. Or be less private and I feel like any time I look at it I am trying to reign it in.”

I: “What didn’t you like?”

P: “I feel like the point of Facebook is to be open, so I’m not exactly upset with them about it... but I just don’t like it very much.” [participant 13]

We used thematic analysis (Braun & Clarke, 2006) on the interviews to extract prevalent themes about privacy from our exploratory analysis. From the thematic analysis we found that our participants talked mostly about the differences in the number of settings (in other words, the granularity of enabled privacy regulation on the applications), confusion, and control over their information. A more detailed explanation of the themes follows here.

Changes

In spite of indicating that settings matched expectations, a majority of participants changed something (unprompted by the Investigator) during the session (12/20). Three of those who did not change anything said they intended to go back to change something specific. Out of the total participants (regardless of whether they changed anything or wanted to change anything), many also indicated they wanted to go back to read more about settings, though they also admitted they were not sure they would ever get around to doing so (14/20). At first it might appear that points 1 and 2 are in some conflict (people’s
expectations are met yet they change settings), but this can be explained by the overall low expectations people have. Some even mentioned that they have no expectations or that they are not happy with social media, but view it as an inevitability (our word).

That Twitter may have had such different results in the above scales was in part explained by our participants’ discussions of the changes they made to their settings. For instance, this participant said he wanted to be notified of changes to default settings and options. This is a typical example of why people changed settings to update them since they had lasted checked.

I: “So I think there were three things you changed, can you tell me more about why you did so?”

P: “Sure. I think they amended some of their options from the last time I looked at it. So the personalization and Twitter content tabs were what I altered, which tailors Twitter based on my recent information shared by content providers. The reason I changed those is that I want my Twitter feed to be only the content I personally have selected and that I want to see, and I don’t want it flooded with suggestions and ideas that Twitter or advertisers may want me to see.” [participant 11]

The following participant expressed how he perceives Twitter differently from other platforms:
P: “With Twitter I expected to want it to be more private, but I was actually more surprised at how many settings I wanted to change on Twitter. I think that Facebook is more open about their lack of concern for my privacy, whereas with Twitter I don’t know what their company line is. I know they need people to connect but I think Facebook is more open about it. It doesn’t necessarily do them favors. It means that I trust Twitter more and maybe I shouldn’t.” [participant 13]

Granularity

Facebook and Google+ have layers of settings, while Instagram only has “private” or “not.” Pinterest and Twitter are somewhere inbetween. Some of our participants volunteered that they prefer for the latter (simpler settings) although we did not specifically ask about this. People said that they use Facebook and Google+ very differently from how they use the other platforms. As generally expressed by our participants, three platforms (Twitter, Instagram, Pinterest) were meant to be a public place for them to broadcast thoughts, opinions, jokes, or work-related communications, while the other two have much more complex purposes.

The purpose of the platform is clearly important; some applications are used mostly for public broadcasts, while Facebook in particular is much more complex in terms of what
people use it for, like this participant, who reflected what many of our participants said about the simpler platforms:

P: “The reason I have a Twitter account is to share it with groups of people. I usually have other messaging – if I want to do – you know, Whatsapp or something else like direct messages.” [participant 11]

Confusion: readability and usability

Related to the above, most interview participants expressed that they did not understand what one or more of the settings were for (17/20). This confusion was not exclusive to a particular platform (that is, one or more people expressed confusion about something on every platform measured).

Commonly, our participants said they were confused about what settings did. Several of them also talked about slips they made when using Facebook (they knew what they wanted to do, but accidentally did something wrong in spite of their knowledge).

For example, our participant who extensively used private groups discussed a time he posted something to his main timeline instead of to one of the private groups:
P: “I wish you could set something so you could tell which part of Facebook you are on. It all looks very similar... so if you could change the background color or something that might help.”

I: “Is that because, well, you said you once posted something to the wrong group...?”

P: “Yeah... I mean if I had scrolled up then I would have seen where I was, but if there had been... like a bigger.... I have this issue a lot. I subscribe to so many of these groups that sometimes it’s not clear if I’m on the private group or if I’m on my newsfeed.” [participant 1]

Control

In accordance with theories about privacy that regard control over information as a key part of personal privacy (Moor, 1997), our participants employed a variety of strategies for curating and their information in order to control their self-presentation. Most of these strategies involve work-arounds of the technological features of the applications.

- Citing social awkwardness, only one participant expressed denying friend requests or blocking follows from people they had met face-to-face (1/20). Although a few said they accept friends and then delete them later in the hopes the person will not notice, the large majority accept everyone.

- Only two participants used the built-in “circles” to manage acquaintances (one on Facebook and one on Google+). One additional participant used a private group on Facebook to post topic-specific content to particular friends without sharing it with
others. Other than these three (out of 20), the remaining participants talked about other strategies for controlling their personal information, that did not utilize the technological ability of the tool at hand. The reason for this is likely the cognitive complexity and work that is required to manage friends and circles.

Control through friend curation and application-enabled friend groups (e.g. “circles”)

P: “I have received innumerable friend requests from people I don’t know who may or may not be actual people. Universally I just don’t add them.” [participant 11]

Our participant who expressed that she did the most work to curate her “friend circles,” also stated that she did not usually delete things because she had mostly friends who posted agreeably on her timeline.

P: “If someone was... you know a huge fan of [a particular presidential candidate], and posted something about how great he was... then I would probably delete it, you know? But my friends aren’t likely to do that.”

Yet the same participant stated that she accepts most requests:
P: “Despite the fact that I keep my Facebook like, locked down, it would be quite easy for someone to become my friend because if someone requests me then I am likely to accept ... because of the social pressure.” [participant 9]

Control through work-around strategies for curation

The simplest work-around strategy was non-use. Four participants mentioned that they have at one time or another “deleted” their accounts or simply stopped using particular social media in order to avoid the work required to curate their friends and content. Others talked about not posting publically, and only using the private message options just as a means to find an old friends' contact information. One example quote was: “Yes, I would like to be able to delete my account [on Facebook],” in reference to what he’d like to change.

For example a few of our participants explicitly spoke about “taking a break” from Facebook. They discussed the amount of work required for proper upkeep, as well as loss of trust due to popular articles or just a general feeling of distrust for one reason or another for Facebook in particular. For example this participant touches on both aspects (trust and workload):
P: “My logging on dropped off significantly after the emotional manipulation article. I stopped using it entirely for about 6 months after that. I found that incredibly disturbing, just that aspect really bothered me. I found it offensive. There’s too many people being, you know, bullied on social media and on Facebook especially. There’s a lot of verbal violence that goes on, and doing something that contributes - I found the data fascinating, but I was bothered by the fact that they did the study at all. I check it maybe monthly now to keep up with relatives that don’t live nearby and [identifying names] but I found that it was extremely time consuming when I checked it more, and I don’t miss that.” [participant 6]

Another final strategy was deletion. Nine participants said they delete things in order to maintain a particular online persona (our word). Sixteen participants said they delete things but only if there is a typo or mistake - a kind of deletion that is conceptually different. Reasons for deleting to maintain identity included removing offensive, controversial, and embarrassing material. Example quote: “Whether I agree or not I just don’t want anything political there.”

Participants deleted content on Facebook more than any other platform. On Twitter, the next most-used application we studied, participants rarely if ever deleted, and then only for typos or similar mistakes. The two participants below both illustrate the nuanced reasons they would want to delete content for reasons other than simple typos or mistakes.
P: “I’ve deleted pictures of me and ex-boyfriends, pictures that are unflattering .... I went through and protected ... back in the day I just posted everything - all my photos from early college. I went through and locked all of those. I didn’t get rid of them but nobody can really see them anymore ... or my Aunts will post on my wall and use a pet name, and I’m like this is public, so I’ll hide that or delete that ... anything embarrassing.” [participant 5]

P. “Whether I agree or not I just don’t want anything political there so I try and minimize people tagging me on anything that way I don’t have to worry about it .... If I were in the same room as them it would be one thing, but just throwing it out there on the Internet is different.” [participant 12]

To sum up, our participants in study 2 talked more about understanding their settings and using easy strategies to curate their content and identities than they talked about using existing technological constraints to manage friends or groups. They expressed a belief that social media is there to connect them to other people and that they want to be connected, but they also expressed a desire for transparency regarding what happens to their content.
Conclusions and Discussion

In this study we wished to investigate, systematically and empirically, whether people are sharing what they think they are sharing online, and how confident they are that they are sharing what they wish to share. Our fundamental research question was, “Do consumers have an accurate perception of their own privacy settings in their social media applications?”

In study 1 we paid 700 crowd-sourced participants to respond to a brief survey about their social media use and their perceptions about their privacy settings. We chose to investigate five popular social media applications: Facebook, Google services (Google+), Twitter, Instagram, and Pinterest.

For four of the applications respondents claimed to change their privacy settings “occasionally” – but for Pinterest the median response was “not at all.” This fits with our finding that in Pinterest only 54% of the respondents were “confident” or “strongly confident” they knew where to locate the privacy settings, whereas the other four applications yielded between 70 and 87% responses in the combined “confident” and “strongly confident” categories.

One potentially interesting finding was that while Facebook yielded the highest percentage of people who were confident or strongly confident they knew where the privacy settings were (87%, with Google+ being in second place with 79%) , Facebook yielded only the third highest confidence (74%, to the Google+ 81%) that the settings were as intended.
Study 2 consisted of one-on-one interviews with 20 social media users. In general participants are not surprised by their settings on most platforms. On a scale of 1 to 10, with 10 being “exactly matched my expectations,” median responses were:

- Instagram: 9
- Facebook: 8.2
- Pinterest: 8
- Google+: 7
- Twitter: 3

So, with the exception of Twitter (though the N was small for Twitter, with only 4 of our 20 interviewees being Twitter users), most study 2 participants expressed that their privacy settings pretty well matched what they had intended them to be. Now, survey and other self-report data are subject to response bias – users get to tell us what they wish to tell us, and we have little way of determining if these responses are accurate. Plus, there may well be a tendency to try to reflect oneself in the best light; our interviewees may not have wished to admit to us (or even to themselves!) that their understanding of their privacy settings was wrong. But compare with these relatively strong reports of matched expectations these two observations:

- most interview participants expressed that they did not understand what one or more of the settings were for (17/20)
- perhaps most interestingly, we found that 75% or our interviewees changed something (12/20) or asserted that they were going to (3/20), unbidden by the
Investigator. That they did so suggests that they were displeased with their settings in one or more cases, even if they said that their expectations were met.

Fundamentally, we find social media users sanguine about privacy – our participants expressed low expectations about their ability to track changes in privacy policies, yet relatively strong confidence that they knew where to locate the privacy settings and set them as they intended. However, when invited to investigate their own settings, three-quarters of our interviewees made changes or expressed a desire to do so. We conclude that people’s privacy settings tend not to be what they think they are (or wish them to be). We would hope our follow-on study would be a systematic A|B study of the usability of privacy settings UIs, including consideration of various ways to visualize those settings to maximize users’ understanding of them.

**Budget**

<table>
<thead>
<tr>
<th></th>
<th>Projected</th>
<th>Actual</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. PI, two summer months’ salary:</td>
<td>$22,000</td>
<td>$22,000</td>
</tr>
<tr>
<td>b. 20-hour/week GRA ship across the summer</td>
<td>$ 8,000</td>
<td>$ 8,000</td>
</tr>
<tr>
<td>c. Samuel Burns, IT consultant</td>
<td>$ 1,000</td>
<td>$ 1,000</td>
</tr>
<tr>
<td>1. Test subject remuneration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Study 1, 1000 participants @ $1.40 each</td>
<td>$ 1000</td>
<td></td>
</tr>
<tr>
<td>(Actually, 700 participants: $700 went directly to participants, $280 to Amazon Turk.)</td>
<td>$ 980</td>
<td></td>
</tr>
<tr>
<td>Study 2, 40 participants @ $50 each</td>
<td>$ 2000</td>
<td></td>
</tr>
<tr>
<td>(Actually, 20 participants)</td>
<td></td>
<td>$ 1,000</td>
</tr>
<tr>
<td>d. Total</td>
<td>$34,000</td>
<td>$32980</td>
</tr>
</tbody>
</table>
References


Appendix A: Introduction to the Survey

We would appreciate your assistance with this research project on social media privacy settings. This research will help us understand your expectations and preferences about privacy.

All you need to do is complete this short questionnaire, which should take approximately 10 minutes. If you do not wish to participate, simply discard the questionnaire or select "no" below.

In order to complete the survey you must be 18 years old.

Responses will be completely anonymous; your name will not appear anywhere on the survey. Completing the questionnaire constitutes your consent to participate.

If you have any questions regarding the research, contact Ramona Broussard, School of Information, 512-433-9247, ramonab@utexas.edu. Dr. Randolph Bias is the advisor on this project. If you have any questions regarding your rights as a research participant, please contact the Institutional Review Board office at the University of Texas. Thank you again for your help.

Appendix B: Survey Questions

Do you identify as...

- Male
- Female
- It's complicated
- Decline to answer

Where do you currently reside?

How old are you?

What do you estimate your household income is? (go ahead and include any residents of the place you consider home)

I consider myself technologically savvy.

- Strongly Agree
- Agree
- Neither Agree nor Disagree
- Disagree
• Strongly Disagree

If you have 10 dogs and you take away 8, how many dogs do you have?

• 1
• 2

Which of the following social media platforms do you have an active account on? (Select as many as you like, we'll assign you questions about only 2 of them).

• Google+
• Twitter
• Facebook
• Instagram
• Pinterest

Please select the “three” below for this question.

• 1
• 2
• 3

Which of the following best reflects how often you use [randomly assigned platform]?

• Less than twice a month
• 2-3 Times a Month
• Once a Week
• 2-3 Times a Week Daily (or more)

How often do you change your account settings in [randomly assigned platform]?

• Not At All
• Occasionally
• Frequently

Who do you share content with on [randomly assigned platform]?

• Everyone
• Just my friends
- Friends and their friends
- No one
- Other (please explain)

How confident are you that you know where to find your privacy settings in [randomly assigned platform]?
- Strongly Confident
- Confident
- Neither confident nor unconfident
- Only slightly confident
- Not at all confident

How confident are you that your privacy settings on [randomly assigned platform] allow you to share content only as you wish?
- Strongly Confident
- Confident
- Neither confident nor unconfident
- Only slightly confident
- Not at all confident

Has anyone else ever shared something about you that you wish they hadn't on [randomly assigned platform]?
- Yes
- Not sure
- No
- Other (please explain)

Have you ever accidentally shared content on [randomly assigned platform] that you wish hadn't been shared?
- Yes
- No
- Other (please explain)
Appendix C: Interview Consent Text

The researchers for this study are:

Conducted by Randolph Bias, PhD, Professor
School of Information, The University of Texas at Austin
1616 Guadalupe
Austin, TX 78701-1213

Ramona Broussard, MSIS, PhD Student
School of Information, The University of Texas at Austin
1616 Guadalupe Suite #5.554
Austin, TX 78701-1213
512-433-9247
ramonab@utexas.edu

The purpose of this study is to learn about privacy and social media. If you choose to take part, we will ask you to:

- Provide some demographic information about yourself and finish a short survey.
- Walk through privacy settings on one or two social media platforms.
- Answer a few questions regarding your experience.

We expect that it will take about one to one and a half hours of your time to complete all the tasks and the questionnaires. You can contact the researchers at the above address, email address, and phone number to discuss the study. The risks of participating in this study are no greater than everyday life. There are no costs for participating. You will not directly benefit from participating. Your identity will not be recorded; researchers will use a pseudonym or fake name for you in the research records. The interviews will be audio recorded with your permission. The recordings will be coded so that no personally identifying information is visible on them or in the file name. The audio files will be replayed only for research purposes; their contents will be viewed only by the investigators and the files will be erased after they are transcribed and coded.

Your participation in this study is voluntary. You may decide not to participate, choose not to answer any question, or stop participating at any time without any penalty. If you want to withdraw from the study or have any questions, contact the investigator listed above.
Appendix D: Interview Questions

- On a scale of 1-10, how closely did your settings match what you thought they were?
- How long have you been using [social media platform 1]? What about [social media platform 2]? How often do you post, versus just logging in?
- Walk me through the last time you posted on [social media platform 1]. What about [social media platform 2]? [Allow them to expand about settings: If they use Facebook, also ask about geolocation, for example, if they use Twitter, ask about direct messaging (do they use it?)
- Did anything you just saw in your settings surprise you? [Repeat for both accounts] (If so what?)
- Have you ever been surprised by how much exposure you got for a post (can you think of a recent example?). Have you ever been disappointed by how little exposure something got?
- Have you ever been surprised by someone contacting you to add you as a friend? Have you ever been frustrated trying to find someone else?
- Have you ever deleted anything? Why?
- After today, would you change any of your settings?
- Is there anything you wish you could do with your settings that isn’t possible (or you just don’t know how to do?)
- Is there anything else you want to tell me about your privacy settings that I haven’t asked about (or anything from the survey you want to expand on?)? Do you have any questions for me?

Appendix E: New Identity Literacy Survey

Section A: PII (Personally Identifiable Information) Awareness
7-point Likert-type scale (1 = “not at all sensitive” to 7 = “highly sensitive”)
“Stable Characteristics” (9 items)

First Name
Hair Color
Middle Name
Eye Color
Sex
Marital Status
Race/Ethnicity
Job Title
Height
“Contact Information” (5 items)

Last Name  
Phone Number  
Home Address  
E-mail Address  
Zip Code

“Credentials” (5 items)

Social Security #  
Bank Account #s  
Driver’s License #  
Passwords  
Credit Card #s

“Behavioral Data” (5 items)

Credit Rating  
Medical History  
Salary  
School Transcripts  
Online Search History

“Common Authentifiers” (2 items)

Mother’s Maiden Name  
Date of Birth

Section B: Prevention Awareness

7-point Likert-type scale (1 = “not at all effective” to 7 = “highly effective”)

“Data Elimination Strategies” (6 items)

Shred Receipts  
Erase Hard Drives  
Carefully Read Privacy Policies  
Update Software Versions  
Opt Out of Share PII Agreements  
Install Anti-Virus Software

“Disclosure Avoidance Strategies” (6
items)

**Personally Place Paper Mail in Mailbox**
**Have Checks Sent Home**
**Don’t Use Simple Passwords**
**Don’t Use Public WiFi Networks**
**Share SSN Only with Close Family/Friends**
**Don’t Carry Medical Insurance ID on Person**

“Data Protection Strategies” (6 items)

**Financial Documents in Lockbox**
**Share Health Info with Caution**
**Do Not Click on E-mail Links**
**Remove Paper Mail from Mailbox**
**Provide PII Only Through Encrypted Sites**
**Regularly Order Credit Reports**

**Section C: Confidence about Privacy Settings**

7-point Likert-type scale (1 = “not at all confident” to 7 = “highly confident”)

Subjects will be asked these four questions about each of whatever subset of these products they use:
- Facebook
- Google services
- Twitter
- Apple cloud
- Pinterest
- Dropbox
- Snapchat

Confidence about settings (4 items)
*Your personal information is being protected*
You are aware of your current privacy settings

You know who (what groups of people) can gain access to your pictures or other items you share

You understand what parts of your information may be shared with a third party (beyond the application you are using)