On a Scale from 1 to 10, How Private Are You? Scoring Facebook Privacy Settings

Tehila Minkus
Computer Science and Engineering
NYU Polytechnic School of Engineering
tehila@nyu.edu

Nasir Memon
Computer Science and Engineering
NYU Polytechnic School of Engineering
memon@nyu.edu

***Abstract*—As social interactions increasingly move to Facebook, the privacy options offered have come under inspection. Users find the interface confusing, and the impact of the individual settings on a user's overall privacy is difficult to determine. This creates difficulties for both users and researchers: users cannot gauge the privacy of their respective configurations, and researchers cannot easily compare the degree of privacy encapsulated in different users' choices. In this work, we suggest a novel and holistic measure for Facebook privacy settings. Based on a survey of a sample of 189 Facebook users, we incorporate appropriate weights that combine the different options into one numerical measure of privacy. This serves as a building block for measurement and comparison of Facebook users' privacy choices, enabling new inferences and insights.**

I. Introduction

Facebook usage is growing, both in terms of total users and the amount of time spent by users. In September 2012, the total number of users passed the billion-user threshold [1]. On average, these users spend more than seven hours a month using Facebook [2]. As such, Facebook is an important sociotechnical phenomenon worthy of much study.

In particular, privacy is front and center among the challenges facing Facebook users. Many questions demand attention from privacy-conscious Facebook users: How much information should they share, and with whom should they share it? How visible should their profiles be? Users are faced with a large number of choices to make, and the impact of each choice on their overall privacy is not readily apparent.

The current settings are not only confusing to users; they also make it difficult for researchers to objectively compare the privacy of different configurations. In order to draw inferences about users' preferences or to make recommendations for privacy design, researchers need a way to measure just how private the given choices are. Facebook privacy profiles currently involve 17 different settings, making it hard to objectively judge the privacy of any individual profile. For example, how private is a Facebook account where the user's posts are public but his page is not available on search engines? Is it more or less private than another account, where the user's posts are only shown to her friends but anyone can post to her timeline? These questions are very subjective and difficult to answer definitively.

In addition to the different options available across the privacy settings, some settings can expose more sensitive information than others, thus posing greater privacy risk to the users. The challenge is to construct a measure that conveys the impact of one's privacy choices, taking into consideration the available options and the appropriate weights.

A holistic privacy metric can be useful to both users and researchers. From the user perspective, a simple "privacy score" (along the lines of a credit score) could demonstrate how high one's privacy risk is. This would facilitate better-informed decisions about exposing or hiding information. From the researcher perspective, a simple numerical attribute describing a user's privacy settings would allow inferences and comparisons for machine learning or statistical inferences for better privacy design.

In this paper, we construct a weight schema for Facebook privacy settings using two measurable variables: *sensitivity* and *visibility*. Via an online survey, we asked Facebook users to judge the sensitivity and visibility of each option in the Facebook privacy settings. We present the results of 189 respondents. The analysis shows that users perceive different levels of privacy risk in the various Facebook privacy setting. We incorporate the users' judgments into our framework for generating a privacy score based on a user's privacy setting configuration. This serves as a springboard for suggestions for the design of Facebook's privacy interface.

The main contributions of this paper are the following:

- **Measure the importance attributed to different privacy settings by Facebook users.** Facebook offers many privacy settings, ranging from tags to ads. Are all privacy options equally important to users' perception of privacy? We explore this question through a survey of Facebook users and use their responses to rate the different privacy settings on scale of user-perceived importance.
- **Propose a framework and technique for measuring privacy of settings selected by users.** The degree of privacy in a given Facebook profile is a product of all the settings chosen, expressed in a single numerical measure. We elaborate our method for scoring privacy settings,

USEC '14, 23 February 2014, San Diego, CA, USA

http://dx.doi.org/10.14722/usec.2014.23013

using the key attributes of sensitivity and visibility. We believe that our proposed technique can be used as a reference point by other papers as well.
- **Propose new Privacy Shortcuts to ease usability.** We suggest a redesign of Facebook's Privacy Shortcuts feature, where more prominence is given to the privacy settings that people find important. We examine the current privacy shortcuts of Facebook, identify their weaknesses, and nominate new ones based on our survey results.

II. Related Work

A. The Difficulty of Facebook Privacy

Facebook privacy settings are notoriously difficult to navigate: Liu et al. [3] found that 67% of the time, users expressed sharing preferences for photos that were different than their actual settings. Wang et al. [4], in a study of users' regrets on Facebook, reported that users found the interface confusing and misleading. In some cases, this led to privacy breaches of an embarrassing and sensitive nature. Egelman et al. [5] evaluated the usability of Facebook privacy settings by asking users to change them based on some realistic scenarios. The results showed users had difficulties with choosing the proper Facebook privacy settings. Work has also shown the discrepancy between users' sharing intentions and real Facebook privacy settings [6].

The opacity of Facebook's privacy settings was highlighted in the popular press when Randi Zuckerberg, sister of Facebook founder Mark Zuckerberg and former Facebook executive, inadvertently shared a private family photo with some journalists due to some confusing privacy settings [7]. In part, this can be attributed to the fact that users have no way of judging quite how permissive their privacy settings are, or what risk is entailed by each privacy choice they make.

B. Measuring Privacy

Some approaches towards measuring privacy have centered on content or audience instead of the explicit privacy settings. For example, PrivAware measures the privacy risk engendered by a user's friends who may cause side-channel information leakage [8]. Privacy Nudges, a project of Wang et al. [9], also measures privacy risk on a post-by-post basis in order to warn users if they are about to post something they may later regret.

Likewise, Profile Watch provides a web service [10] where users can check what they are sharing publicly on Facebook. The output is a privacy score ranging from 0 (exposed) to 10 (safe). It is similar to the "View as" tool provided by Facebook [11]. However, the algorithm used is not public. Additionally, it is not related to privacy settings, and it is not obvious how a low score can be fixed.

Few attempts have been made to create a system that can encapsulate a user's privacy settings in a numeric form. Gjoka, et al. [12] propose a simple method where four bits are used to signify the user's choices for some basic privacy settings. They then use this four-bit data structure to compare privacy across different populations. However, this binary approach fails to capture the different gradations of privacy available to the Facebook user (i.e. friends, friends-of-friends, friends-except-acquaintances, everyone) and instead measures only whether a user has conformed to the default settings.

The closest work to ours is that of Maximilien et al. [13]. They propose a platform for online data sharing called Privacy-as-a-Service, where users determine their access control by determining the privacy characteristics of each settings. As the basis for these decisions, they focus on data's sensitivity and visibility. They combine these measures to create a "privacy index" expressing the privacy risk of sharing specific data. We use this as a basis for our approach, with several important distinctions. While [13] suggests a data access framework, we propose an analytic tool to assign metrics to existing privacy settings. Instead of mediating data access, we aim to facilitate research and analysis of existing data access rules. This is enabled by a holistic privacy metric rather than a data sharing framework. Secondly, instead of requiring each user's privacy risk variables to be chosen on an individual basis, we conduct a survey and collect aggregate values to facilitate large-scale application of the techniques introduced.

III. Methods

In this section, we present two approaches to scoring user privacy settings. The first method requires no a priori knowledge of users' privacy perceptions; it is based purely on the options made available in the interface. The second method takes into account the importance placed by users on each option in the privacy setting interface. These weights are incorporated into the score to represent the degree of privacy encapsulated in a given configuration of privacy settings. We believe that the weighted method best encapsulates the importance of each privacy setting.

A. Notation

Before explaining the scoring methods, we will introduce some brief notation.

We will refer to the list of privacy settings as C. To refer to the privacy setting at position i, we use C_i; so, for example, C_1 = "Who can see your future posts?" Refer to Table I for a list of current Facebook privacy settings and corresponding positions.

To refer to the specific privacy settings chosen by user x, we use $C(x)$. $C(x)$ represents a vector of options that user x has chosen for each privacy setting. Thus, $C(x)_i$ represents the specific choice that user x chose for privacy setting C_i.

For each setting on Facebook, there are several options available (e.g. "friends", "friends of friends", "public"). Each of these options has a specific privacy rating. We refer to each of the j options available for setting C_i as $C_{i,j}$.

By way of clarification, let us introduce the hypothetical user Laura. $C(Laura)$ would be the settings that Laura chose as her privacy settings on Facebook. For the first privacy setting, Laura has chosen the option "Only me." So, $C(Laura)_1$ = "Only me".

If user x has chosen option j for setting C_i (in notation, $C(x)_i = C_{i,j}$), we refer to the privacy rating for this option

Privacy	Timeline and Tagging	Apps	Ads
1) Who can see your future posts? 2) Who can send you friend requests? 3) Whose messages do you want filtered into your inbox? 4) Who can look you up using the email address or phone number you provided? 5) Do you allow other search engines to link to your timeline?	6) Who can add things on your timeline? 7) Review posts friends tag you in before they appear on your timeline? 8) Who can see posts you've been tagged in on your timeline? 9) Who can see what others post on your timeline? 10) Review tags people add to your own posts on Facebook? 11) When you're tagged in a post, who do you want to add to the audience if they aren't already in it? 12) Who sees tag suggestions when photos that look like you are uploaded?	13) What personal information goes into apps others use? 14) What is instant personalization set to? 15) Who can view your posts from old versions of Facebook for mobile?	16) Ads shown by third parties. 17) Ads and friends.

TABLE I
CURRENT FACEBOOK PRIVACY SETTINGS, DIVIDED IN FOUR CATEGORIES.

as $s(C(x)_i)$. It can also be referred to as $s(C_{i,j})$). This is the privacy score attained by the choosing that specific setting for the given privacy option.

For each user x, the total privacy score is denoted as $S(x)$. All scores S are normalized on a scale from 0 to 10 for ease of comprehension. A user who has totally public settings would receive a score of 0, and a user with maximally private settings should receive a score of 10.

B. Naive Scoring Method

As a baseline, we propose a naive scoring method to enable comparison between different users' Facebook privacy settings. Simply stated, for each question, the least private option receives a mark of 0, and each successively more private option receives a score incremented by 1.

The following algorithm outputs a privacy rating $s(C_{i,j})$ for each option j in a privacy setting i.

```
algorithm NaivePrivacyRating (setting)
    Sort options of setting from least private
        to most private
    Set currentScore = 0
    For each option in sorted options:
        assign currentScore to option
        increment currentScore by 1
    Output a dictionary of options along with
        their score
```

The overall privacy score consists of the sum of all the privacy settings' scores.

The total score of a user is calculated as the sum of the scores of each options. Using our above notation, this can be expressed by the following equation, where n is the total number of privacy settings (currently n = 17) and j is the number of options available for a specific setting:

$$S(x) = \sum_{i=1}^{n} \frac{s(C(x)_i)}{\max\limits_{k} s(C_{i,j})} \tag{1}$$

In summary, choosing more private options will produce a higher score, while lower scores imply less private settings. All settings are given equal weight by this method.

1) Advantages of the Naive Approach: This method has the advantage of simplicity; it requires no a priori knowledge of the data or of users' perception of privacy risks on Facebook. It can be easily calculated and explained.

2) Disadvantages of the Naive Approach: This approach suffers as a result of this very simplicity. Namely, it rests upon the assumption that each privacy setting has equal bearing upon privacy. This, however, is a mistaken assumption; some settings are clearly more wide-ranging than others. Each setting does not necessarily entail the same extent of personal information exposure. For example, score 0 for one setting may mean that "Everyone" can see this particular piece of information, while for another setting may mean "Only my Friends". And conversely, score 1 may stand for "Friends", "Friends of Friends", or "No one" depending on the context of the setting. Thus, significant differences may exist between accounts with identical scores, since users may be very private in certain categories of privacy settings and yet quite public in others.

C. Weighted Scoring Method

We introduce a more sophisticated alternative, which we deem the weighted method. Instead of considering all settings to be equally important in regard to privacy, the weighted method considers each question's privacy-breach potential when calculating its impact on the final privacy score. A setting's weight is determined by two key features, sensitivity and visibility.

Our approach is similar to that of the Privacy-as-a-Service model introduced by Maximilen et al. [13]. We focus particularly on Maximilien et al.'s emphasis on two traits as measures for privacy risk: *sensitivity* and *visibility*:

- **Sensitivity** is a measure of how private or embarrassing the information in question may be.
- **Visibility** is a measure of how public the information would become in the situation of a breach.

High sensitivity means that showing the information would be very embarrassing, while high visibility would mean that a

lot of people could see it. As an example, consider different mediums of communication: a newspaper has high visibility, and a private letter has high sensitivity. On Facebook, a specific privacy setting may have any combination of visibility and sensitivity. For example, the setting “Who can see your future posts" has potentially high visibility, and the setting “Do you want to share your birthday with apps” (paraphrased) is a high-sensitivity question, considering the fact that one’s date of birth can serve as identifying information.

The privacy score, s, of each setting is calculated as shown in the above algorithm (see Section III-B). The next step is determining the weight of each setting.

Once values have been determined for each setting’s sensitivity and visibility, the setting’s weight in the privacy score is determined by calculating the product of its sensitivity and visibility ratings (as shown in [13]). We refer to the weight of a given setting as $w(i)$, where i is the index of the given setting in the settings list and shown in Table I. The weight is expressed as follows:

$$w(i) = sensitivity(i) * visibility(i) \quad (2)$$

The overall privacy score of individual x’s privacy settings can be computed as follows:

$$S(x) = \sum_{i=1}^{n} s(C(x)_i) * w(i) \quad (3)$$

Intuitively, this expresses that settings with greater perceived privacy risk have a larger impact on the overall privacy score of the given configuration.

IV. Survey

A. Survey Design

In order to determine the weights for each privacy setting, we submitted a survey to Facebook users through the Amazon Mechanical Turk marketplace. Responses were restricted to the United States to maintain a consistent sample. In order to ensure accurate answers, we followed standard best practices such as inserting attention-gauging questions and completion codes [14]. We paid each subject $0.30 for answering a total 26 questions, divided into three parts:

1) Demographic Information: The respondents were asked for basic demographic information, i.e. gender, age, and highest level of education completed.

2) Description and Definitions: Respondents were asked to carefully read the description of the survey and definitions of sensitivity and visibility and acknowledge that they understood the terms before continuing.

3) Rate Facebook Privacy Settings: This part consisted of 19 questions, including two attention-measuring questions. The remaining 17 questions listed the privacy settings along with their available options. When the privacy setting was not self-explanatory, we provided a brief description. (This was the case in the settings for the “Apps” and “Ads” categories shown in Table I). Each question asked respondents to rate the privacy setting on a 5-point Likert scale by asking “How sensitive is this?” and “How visible is this?”. (Due to space constraints, we can not include a copy of the entire survey.)

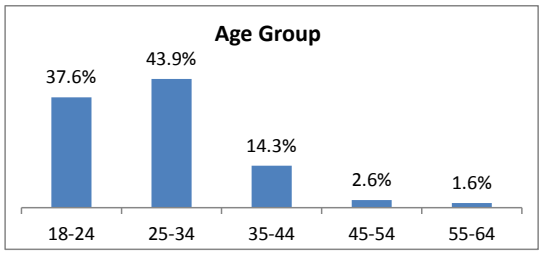

Fig. 1. Age of respondents.

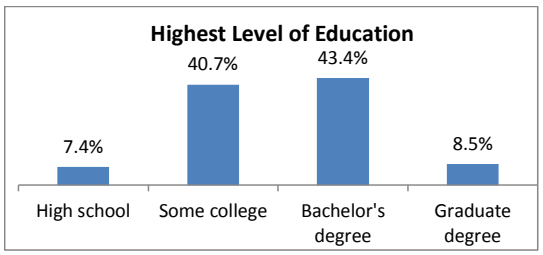

Fig. 2. Highest level of education respondents have completed.

B. Dataset

Of the 250 responses we had requested, 61 respondents failed to select the correct answers to the attention-measuring questions incorporated in the survey. After removing those responses from analysis, there were 189 responses remaining. 35.4% of the respondents were females and 64.6% males. Based on demographic statistics of 2012 [15], more Facebook users are female (55%) than male (45%), indicating that females are underrepresented in our sample.

The age groups encompassed ages 18 through 65. A detailed breakdown is in Figure 1. Our sample follows the same pattern with the general population of Facebook users [15], with 18-24 and 25-34 as the dominant age groups. Education levels are shown in Figure 2.

C. Results

The responses confirmed our hypothesis that all privacy settings are not created equal. There was considerable variance among the ratings for different options. For example, users on average rated the sensitivity of the "Who can send you friend requests" setting as 1.09, but "What personal information goes into apps others use" scored 2.82 for sensitivity - more than double as sensitive. For visibility, average assigned values ranged from 1.47 ("Whose messages do you want filtered into your inbox") to 2.59 ("Who can see what others post on your timeline"). All ratings were on a scale from 0 to 4. Overall, users displayed a keen understanding and belief that different settings have disparate impacts on their overall privacy.

A full listing of each setting’s sensitivity and visibility ratings can be seen in Table II. The final privacy score, calculated as the product of the sensitivity and visibility values, as suggested in [13], is also included.

We also examined the relationship between sensitivity and visibility. The majority of privacy settings exhibited similar

Privacy Setting	Sensitivity	Visibility	Sens.*Vis.
What personal information goes into apps others use?	2.82	2.16	6.0912
Who can see what others post on your timeline?	2.17	2.59	5.6203
Who can see posts you've been tagged in on your timeline?	2.39	2.35	5.6165
Who can look you up using the email address or phone number you provided?	2.42	2.17	5.2514
Who can add things on your timeline?	2.16	2.32	5.0112
Who can see your future posts?	1.97	2.41	4.7477
Review posts friends tag you in before they appear on your timeline?	2.29	1.96	4.4884
Who can view your posts from old versions of Facebook for mobile?	2.08	2.08	4.3264
When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	1.84	1.94	3.5696
What is instant personalization set to?	2.12	1.65	3.498
Who sees tag suggestions when photos that look like you are uploaded?	1.89	1.79	3.3831
Ads and friends. Pair my social actions with ads for whom?	1.89	1.78	3.3642
Review tags people add to your own posts on Facebook?	1.81	1.77	3.2037
Ads shown by third parties. Show my information to whom?	1.8	1.76	3.168
Do you allow other search engines to link to your timeline?	1.86	1.63	3.0318
Who can send you friend requests?	1.09	2.04	2.2236
Whose messages do you want filtered into your inbox?	1.47	1.47	2.1609

TABLE II
WEIGHTS OF CURRENT FACEBOOK PRIVACY SETTINGS, SORTED BY THE PRODUCT OF SENSITIVITY AND VISIBILITY IN AN INCREASING ORDER.

levels of sensitivity and visibility; however, three settings showed significant differences in their respective ranks for privacy and sensitivity.

"Who can see your future posts?" scored ninth in sensitivity while ranking second in visibility. This option can have very public consequences, but users did not seem to think that very sensitive information would be leaked in that case. "What is instant personalization set to?" was seventh in sensitivity ranking and only 15^{th} in visibility. It appears that users perceive instant personalization to be somewhat sensitive but not very public. That may be due to the wording of the definition given, where Facebook states that it will allow personalization with only a few partner companies, constituting a limited audience. The least sensitive option (as rated by users) scored eighth in visibility: "Who can send you friend requests?". Users apparently believe that receiving a friend request is not sensitive, but they recognize that when accepted it could allow some personal information to become visible.

V. DISCUSSION

According to the old business adage, "If you can't measure it, you can't manage it." Research has consistently shown that Facebook users' privacy settings suffer from mismanagement. In this paper, we attempt to alleviate this problem by introducing a measurement that can represent privacy in an informed and well-considered manner. This privacy metric is sensitive to the different levels of privacy importance ascribed to each setting by users. This can be of use to several parties.

A. Benefit to users

Currently, Facebook users receive little feedback when setting their privacy settings. They must choose a privacy configuration without knowing exactly how the settings measure up. By the time users realize they chose unwisely, it is usually too late [4]. Using a framework such as the one proposed, allows users to view their privacy levels on a simple numerical scale and adjust likewise. Users who wish for more open profiles can aim for a lower score, and users who want to retain privacy can tweak their settings to reach a higher privacy score. Just as some social networks in (e.g. LinkedIn) show the percentage of a profile that is complete, this would show how private the profile is.

B. Benefit to researchers

This framework is highly beneficial for researchers who wish to study and compare users' Facebook privacy settings. Until now, there has been no unified approach towards all the privacy settings, forcing researchers to focus on only a few settings in the focus of their research. By combining the settings while retaining their respective importance to privacy, we enable broader and deeper study of users' privacy choices on online social networks.

C. Benefits to Facebook designers

In the course of this work, we analyzed users' perspective on the respective importance of each privacy setting. This data could be incorporated into Facebook, both in philosophy and design, to better facilitate and respect the privacy of users.

One application would be to modify the Privacy Shortcuts on Facebook. At the end of 2012, Facebook introduced Privacy Shortcuts, a privacy settings interface that appears one click away from user's timeline [16]. Among these privacy shortcuts, users can easily find and set some of their privacy settings. Figure 3 shows two instances of privacy shortcuts.

Below, we examine the current privacy shortcuts from a functionality perspective, based on the results of our survey.

"Who can see my future posts?": Our analysis showed that this setting is rated sixth among all for privacy importance. We therefore recommend that it be replaced with a higher-priority setting, as rated by users.

"Whose messages do I want filtered in my Inbox?" and **"Who can send me friend requests?":** Users in our survey rated these questions as the least important among all privacy settings. They were rated as the least crucial both in sensitivity

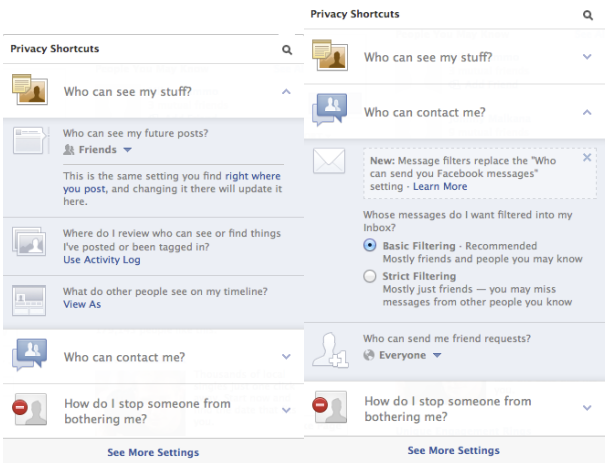

Fig. 3. Facebook Privacy Shortcuts. The left side displays expanded options under "Who can see my stuff?". The right side shows the expanded options for "Who can contact me?"

and in overall privacy importance. Therefore, we question the presence of these privacy settings in the privacy shortcuts.

Based on our survey's results, we suggest new Privacy Shortcuts. We recommend that they comprise the three privacy settings that are among the top five in all categories: sensitivity, visibility, and final privacy score. As presented in Table II, these privacy settings are: 1. "Who can see what others post on your timeline?", 2. "Who can see posts you've been tagged in on your timeline?", and 3. "Who can look you up using the email address or phone number you provided?". This would allow easy access to the settings deemed most important on average.

D. Limitations

The technique proposed above for scoring privacy on Facebook bears some limitations:

- **Platform-specific:** our technique as proposed can only be applied on Facebook's privacy settings. However, the methodology can be easily extended to survey privacy in other online social networks as well.
- **Susceptible to changes:** Facebook updates its privacy settings rather frequently. This would cause the results presented in this paper to become outdated. However, the framework and the technique are generic and elastic and can therefore be easily reapplied to any new privacy settings. We point out that researchers should check our list of settings against the current ones on Facebook and perform a new survey if necessary.

VI. Conclusion

In this paper, we introduce a novel metric to encapsulate the degree of privacy expressed in a Facebook user's privacy settings. This serves as an at-a-glance summary of the user's privacy state. In addition to helping users manage their privacy, it can also help researchers learn about privacy and enable Facebook designers to consider privacy in their work. The privacy score is built by combining the options via weights, which are determined by the sensitivity and visibility of each setting. We conduct a survey of Facebook users to assign the sensitivity and visibility values. Using these values, we present an ordering of the Facebook privacy settings according to user-perceived privacy risk. Finally, we make recommendations to incorporate these principles into the design, usage, and research of Facebook.

VII. Acknowledgements

This work was supported in part by the NSF (under grant 0966187). The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of any of the sponsors.

References

[1] "Number of active users at Facebook over the years," http://finance.yahoo.com/news/number-active-users-facebook-over-years-214600186--finance.html.

[2] "March 2012 - Top Online Brands and Sports Websites," http://www.nielsen.com/us/en/newswire/2012/march-2012-top-us-online-brands.html.

[3] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: User expectations vs. reality," in *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*. ACM, 2011, pp. 61–70.

[4] Y. Wang, G. Norcie, S. Komanduri, A. Acquisti, P. G. Leon, and L. F. Cranor, "I regretted the minute i pressed share: A qualitative study of regrets on facebook," in *Proceedings of the Seventh Symposium on Usable Privacy and Security*. ACM, 2011.

[5] S. Egelman, A. Oates, and S. Krishnamurthi, "Oops, i did it again: Mitigating repeated access control errors on facebook," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2011, pp. 2295–2304.

[6] M. Madejski, M. Johnson, and S. M. Bellovin, "A study of privacy settings errors in an online social network," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on*. IEEE, 2012, pp. 340–345.

[7] C. Matyszczyk, "Randi Zuckerberg loses control on Facebook (and Twitter)," *c|net*, 26th December 2012, news.cnet.com/8301-17852_3-57560888-71.

[8] J. L. Becker and H. Chen, "Measuring privacy risk in online social networks," Ph.D. dissertation, University of California, Davis, 2009.

[9] Y. Wang, P. G. Leon, K. Scott, X. Chen, A. Acquisti, and L. F. Cranor, "Privacy nudges for social media: an exploratory facebook study," in *Proceedings of the 22nd international conference on World Wide Web companion*. International World Wide Web Conferences Steering Committee, 2013, pp. 763–770.

[10] "Profile Watch - What is your online privacy score?" http://www.profilewatch.org/.

[11] "How can I see what my timeline looks like to other people?" https://www.facebook.com/help/288066747875915.

[12] M. Gjoka, M. Kurant, C. T. Butts, and A. Markopoulou, "Practical recommendations on crawling online social networks," *Selected Areas in Communications, IEEE Journal on*, vol. 29, no. 9, pp. 1872–1892, 2011.

[13] E. M. Maximilien, T. Grandison, T. Sun, D. Richardson, S. Guo, and K. Liu, "Privacy-as-a-service: Models, algorithms, and results on the facebook platform," in *Proceedings of W2SP 2009*, vol. 2, 2009.

[14] P. G. Kelley, "Conducting usable privacy & security studies with amazon's mechanical turk," in *Symposium on Usable Privacy and Security (SOUPS)(Redmond, WA)*. Citeseer, 2010.

[15] "Social Media Agencies and Demographic Statistics," http://blackboxsocialmedia.com/social-media-agencies-and-demographic-statistics/.

[16] "Facebook Introduces New, Uber-Simple Privacy Controls," http://lifehacker.com/5970442/facebook-introduces-new-uber+simple-privacy-controls.