How Good Is Good Enough?
The sisyphean struggle for optimal privacy settings

Serge Egelman
University of California, Berkeley
egelman@cs.berkeley.edu

Maritza Johnson
Columbia University
maritzaj@cs.columbia.edu

Abstract
Previous research on interpersonal privacy on social networking websites has pointed to serious flaws in users' abilities to manage their private information, showing discrepancies between stated privacy preferences and expressed sharing policies. Many have attributed this disconnect to shortcomings of the access control interfaces. While these interfaces and the underlying mechanisms certainly need improvement, the lack of discussion regarding metrics or acceptable failure rates implies that the only acceptable solution is one that does not allow any information to be inappropriately shared. In this position paper, we argue that metrics are needed and that at a certain point, some access control mechanisms should be deemed "good enough."

Keywords
Privacy, social networking, Facebook, access control

ACM Classification Keywords
H.5.2 Information Interfaces and Presentation: User interfaces, Evaluation/ methodology

Introduction
Since the dawn of the social networking era, researchers have examined how technology makes managing interpersonal privacy a difficult task [10]. Some researchers have used data mining to examine the extent to which users are currently sharing personal information with others (e.g., [5] or [1]), while others have performed interviews to elucidate users' privacy concerns when sharing information online and to learn of the strategies that are employed to mitigate those concerns (e.g., [12], [11], or [7]). While popular media reports of online privacy seem to have only increased in the past ten years, the availability of access control mechanisms to restrict access to private data have also increased in both availability and adoption.

Research on social networking privacy is trending towards users' ability to adequately use existing access control mechanisms and the appropriateness of the underlying mechanisms to fulfill users' needs. From this research, it would be pure sophistry to argue that the existing privacy settings interfaces are adequately addressing users' privacy needs, however, we contend that the expectations are unreasonably high and unattainable.

In this position paper we examine previous research performed on privacy with regard to social networking websites and their associated access control interfaces. We argue that

much of this work fails to put privacy failures in context and therefore leads the reader to conclude that only a system that addresses every user's unique privacy preferences all of the time will be adequate. We posit that there exists a point where some privacy interfaces may simply be "good enough." To illustrate our point, we discuss familiar scenarios where people fail to manage interpersonal privacy offline, and encourage the community to explore where parallels might exist for online social networks.

User Privacy Concerns

Shortly after Facebook gained popularity as the social network of choice for college students, Acquisti and Gross conducted two studies of a university population and found that even though most people were concerned with online privacy, they shared large amounts of personal information on Facebook [1], and very few people (0.06% of 4,540 users) had changed the privacy settings such that their data was likely being shared with unintentional recipients [5]. Facebook has changed significantly since then (in user base, features, and available privacy settings [3]) and although significantly more users utilize the available privacy settings, researchers continue to identify inconsistencies between users' sharing goals and their privacy settings.

In 2009, Young and Quan-Haase surveyed 77 undergraduate students regarding their Facebook usage and privacy-preserving strategies. They found that 64% claimed to have restricted their profiles to friends, but also that their participants used a combination of strategies (e.g., sending private messages, self-censorship, etc.) [14]. More recently, Stutzman and Kramer-Duffield surveyed 444 undergraduate Facebook users and found that 83% reported altering privacy settings, while 58% specifically reported changing their profiles to be only viewable by friends. They concluded that "we should design ways to facilitate conversations about everyday privacy behaviors" [13]. These and other works go into great depth to uncover possible correlations between use of privacy-enhancing strategies and other factors (e.g., demographics, tie strength, privacy preferences, etc.). However, correlation does not imply causality; we still have a fuzzy picture of why users who claim to value privacy choose not to use privacy controls, or why users sometimes behave in ways that contradict their stated privacy preferences. The leading explanations that researchers have examined are that the privacy settings interfaces are inappropriate for the context of use, users are unaware of the existence of the settings, or that the controls are too complicated for the average user to master.

Measuring the Correctness of Privacy Settings

In order to move forward, we must measure and understand the shortcomings of the existing mechanisms, but research on the topic seems to assume that perfection is the end goal and fails to specify metrics by which the community should measure progress and identify future success. Krasnova et al. sought to create a taxonomy of users' privacy concerns and study how users adjust their behavior based on their concerns [6]. For the purpose of advancing our argument, we focus on the taxonomy of privacy concerns and note the wide assortment of concerns. Many participants were concerned with social threats which existing privacy settings offer paltry protection against, at best.

One frequently reported social threat involved other users posting embarrassing information that the primary user would not have control over. Besmer and Lipford explored this issue as it relates to photo-tagging [2], and Lampinen et al. studied the need for collaborative processes of managing interpersonal privacy [7]. Both papers suggest minor changes to the existing privacy mechanisms to encourage

pseudo-technical solutions to this problem, acknowledging that a purely technical solution may be insufficient. Skeels and Grudin examined how social spheres overlapped when coworkers became friends on Facebook. They found that the privacy controls were inadequate for many users and that a handful went so far as to create multiple profiles [11].

Egelman et al. evaluated the usability of Facebook privacy settings circa June 2010 in an in-lab study that asked the participant to configure privacy settings according to scenarios [4]. Participants attempted the tasks described in the scenarios, and the researchers measured the correctness of the resulting privacy settings. More recent studies measured the correctness of users' actual Facebook privacy settings in terms of their sharing intentions and identified inconsistencies for the majority of participants [9, 8]. Both of these studies fail to address the ultimate goal for this line of research—how do we know when we have found an optimal privacy settings interface? It is clear that any "optimal" solution for a given user base will not protect against inappropriate sharing 100% of the time.

How Good is Good Enough?

While at a party, you gossip with some friends about someone else only to discover that the subject of your conversation is also in attendance at the party and is within earshot. You tell several friends about your plans to switch jobs, only to find that someone has repeated this to another mutual friend who happens to be a current coworker—maybe even a friend of your boss. These scenarios are just two examples of real world privacy "mishaps" that have analogs to privacy slips on social networking websites. There are many more ways in which people can and will fail to control the flow of their private information. These specific examples and many other commonly discussed sharing "problems" on social networking websites are often the result of poor discretion and cannot solely be blamed on poor interface design or a misunderstanding of the available privacy controls. Our point is that privacy settings are certainly responsible for a subset of privacy failures (possibly the majority, though speculating on this is beyond the scope of our position), however, we must accept that an optimal privacy settings mechanism will still be imperfect and will result in some situations where users inappropriately share information with unintended parties.

It is clear that managing interpersonal privacy on social networking websites has come a long way in the past few years. However, researchers continue to point out scenarios in which users' privacy settings do not match their stated preferences. There is an unsaid implication that the technology is largely to blame and therefore the privacy mechanisms need to be improved (e.g., improving the management interfaces, creating better default settings, changing the underlying access control models, etc.). While we believe there is certainly room for technological improvement, expectations for this improvement must be tempered by discussion of what the technology will allow and what problems are more human in nature.

References

[1] A. Acquisti and R. Gross. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Privacy Enhancing Technologies Workshop (PET '06)*, 2006.

[2] A. Besmer and H. Richter Lipford. Moving beyond untagging: photo privacy in a tagged world. In *Proc. of the Conference on Human Factors in Computing Systems (CHI)*, 2010.

[3] d. boyd and E. Hargittai. Facebook privacy settings: Who cares? *First Monday*, 15(8), August 2010.

[4] S. Egelman, A. Oates, and S. Krishnamurthi. Oops, I did it again: Mitigating repeated access control errors on Facebook. In *CHI 2011*, pages 2295–2304, 2011.

[5] R. Gross and A. Acquisti. Information revelation and privacy in online social networks. In *WPES '05: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, pages 71–80, New York, NY, USA, 2005. ACM.

[6] H. Krasnova, O. Günther, S. Spiekermann, and K. Koroleva. Privacy concerns and identity in online social networks. *Identity in the Information Society*, 2:39–63, 2009.

[7] A. Lampinen, V. Lehtinen, A. Lehmuskalli, and S. Tamminen. We're in it together: Interpersonal management of disclosure in social network services. In *CHI '11: Proceeding of the 29th SIGCHI Conference on Human Factors in Computing Systems*. ACM New York, NY, USA, May 7–12 2011.

[8] Y. Liu, K. Gummadi, B. Krishnamurthy, and A. Mislove. Analyzing Facebook privacy settings: User expectations vs. reality. In *Proc. of Internet Measurement Conference (IMC)*. ACM, 2011.

[9] M. Madejski, M. Johnson, and S. M. Bellovin. The failure of online social network privacy settings. Technical Report CUCS-010-11, Columbia University, 2011.

[10] L. Palen and P. Dourish. Unpacking "privacy" for a networked world. In *CHI '03: Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM New York, NY, USA, April 5-10 2003.

[11] M. M. Skeels and J. Grudin. When social networks cross boundaries: A case study of workplace use of Facebook and LinkedIn. In *GROUP '09: Proceedings of the 2009 International ACM Conference on Supporting Group Work*, pages 95–104, New York, NY, USA, 2009. ACM.

[12] K. Strater and H. R. Lipford. Strategies and struggles with privacy in an online social networking community. In *BCS-HCI '08: Proceedings of the 22nd British HCI Group Annual Conference*, pages 111–119, Swinton, UK, UK, 2008. British Computer Society.

[13] F. Stutzman and J. Kramer-Duffield. Friends only: examining a privacy-enhancing behavior in Facebook. In *CHI '10: Proceedings of the 28th International Conference on Human Factors in Computing Systems*, pages 1553–1562, New York, NY, USA, 2010. ACM.

[14] A. L. Young and A. Quan-Haase. Information revelation and internet privacy concerns on social network sites: a case study of Facebook. In *C&T '09: Proceedings of the 4th International Conference on Communities and Technologies*, pages 265–274, New York, NY, USA, 2009. ACM.