**An investigation into facebook friend grouping -** Patrick Gage Kelley, Robin Brewer, Yael Mayer, Lorrie Faith Cranor, and Norman Sadeh

In a series of 46 semi-structured interviews, we investigated how participants group their online friends using four different grouping methods. Our results show that these different mechanisms alter the strategies and groups that users create, that groups created a priori need further refinement before they can adequately address privacy decisions, and that users are adapting their online behavior to avoid the need to specify groups in the current Facebook interface. We conclude with several recommendations that would allow users improved group-based access control.

**Are you close with me? are you nearby?: investigating social groups, closeness, and willingness to share -** Jason Wiese, Patrick Gage Kelley, Lorrie Faith Cranor, Laura Dabbish, Jason I. Hong, and John Zimmerman

With increasingly large friend networks, Facebook users may be losing sight of exactly with whom they are sharing content they post to Facebook. When Facebook released a new privacy interface in sum- mer 2010 they simplified privacy controls; however, group-based permis- sions remain at the core of fine-grained privacy control. In order to use these fine-grained controls, users must be able to accurately and usefully specify friend groups. In a series of 46 semi-structured interviews, we investigated how participants group their online friends using four differ- ent grouping methods. Our results show that these different mechanisms alter the strategies and groups that users create, that groups created a priori need further refinement before they can adequately address pri- vacy decisions, and that users are adapting their online behavior to avoid the need to specify groups in the current Facebook interface. We con- clude with several recommendations that would allow users improved group-based access control.

**The problem of conflicting social spheres: effects of network structure on experienced tension in social network sites -** Jens Binder, Andrew Howes, and Alistair Sutcliffe

We propose that a fundamental property of human psychology, the need to maintain independent social spheres, imposes constraints on the use of social network sites (SNS). We particularly focus on the consequences of visibility of communications across social spheres, and we hypothesize that technological features of SNS may bring social spheres in conflict, thus leading to increased levels of online social tension. A survey study among Facebook users was conducted to test this hypothesis. Results showed that diversity of the Facebook network predicted online tension. Moreover, the number of kin in a Facebook network was a crucial component because it predicted online tension whereas number of work and social contacts did not. Further, evidence was found to support the idea that tension might impose an upper limit on network size. We conclude with a discussion of these findings and describe how they support the thrust of recent modifications to SNS designs.

**Friends only: examining a privacy-enhancing behavior in facebook -** Fred Stutzman and Jacob Kramer-Duffield

Privacy practices in social network sites often appear paradoxical, as content-sharing behavior stands in conflict with the need to reduce disclosure-related harms. In this study we explore privacy in social network sites as a contextual information practice, managed by a process of boundary regulation. Drawing on a sample survey of undergraduate Facebook users, we examine a particular privacy-enhancing practice: having a friends-only Facebook profile. Particularly, we look at the association between network composition, expectancy violations, interpersonal privacy practices and having a friends-only profile. We find that expectancy violations by weak ties and increased levels of interpersonal privacy management are positively associated with having a friends-only profile. We conclude with a discussion of how these findings may be integrated into the design of systems to facilitate interaction while enhancing individual privacy.

**Analyzing facebook privacy settings: user expectations vs. reality**

Yabing Liu, Krishna P. Gummadi, Balachander Krishnamurthy, and Alan Mislove

The sharing of personal data has emerged as a popular activity over online social networking sites like Facebook. As a result, the issue of online social network privacy has received signiﬁcant attention in both the research literature and the

mainstream media. Our overarching goal is to improve defaults and provide better tools for managing privacy, but we are limited by the fact that the full extent of the privacy problem remains unknown; there is little quantiﬁcation of the incidence of incorrect privacy settings or the diﬃculty users face when managing their privacy.

In this paper, we focus on measuring the disparity between the desired and actual privacy settings, quantifying the magnitude of the problem of managing privacy. We deploy a survey, implemented as a Facebook application, to 200 Facebook users recruited via Amazon Mechanical Turk. We ﬁnd that 36% of content remains shared with the default privacy settings. We also ﬁnd that, overall, privacy settings match users’ expectations only 37% of the time, and when incorrect, almost always expose content to more users than expected. Finally, we explore how our results have potential to assist users in selecting appropriate privacy settings by examining the user-created friend lists. We ﬁnd that these have signiﬁcant correlation with the social network, suggesting that information from the social network may be helpful in implementing new tools for managing privacy.

**Sharing ephemeral information in online social networks: privacy perceptions and behaviours** - Bernardo Reynolds, Jayant Venkatanathan, Jorge Gonçalves, and Vassilis Kostakos.

This paper presents a study where the online Facebook practices of a sample of users (n=103) was analysed over a period of two years, via the scraping of data in Facebook and the collection of questionnaire data. The data allows for a contrast between implicit and explicit attitudes regarding Facebook and online sharing. Our analysis reveals that while overall privacy concerns are not reflected in posting behaviour, awareness and familiarity with privacy controls is. This is supported by contrasting users' attitudes regarding day-to-day sharing against actual behaviour on Facebook. We theorise that there exists a failure in translating users' privacy needs into a social-technical environment such as social networking sites. This work demonstrates how aspects such as demographics and usage influence and shape users' behaviour and practices towards privacy. We therefore argue that the factorization of these aspects may augment the translation of users' privacy needs and improve the design of privacy sensitive mechanisms for day-to-day information sharing.

**Facebook Privacy Settings: Who Cares?** - Boyd, D., Hargittai, E.:

With over 500 million users, the decisions that Facebook makes about its privacy settings have the potential to influence many people. While its changes in this domain have often prompted privacy advocates and news media to critique the company, Facebook has continued to attract more users to its service. This raises a question about whether or not Facebook’s changes in privacy approaches matter and, if so, to whom. This paper examines the attitudes and practices of a cohort of 18– and 19–year–olds surveyed in 2009 and again in 2010 about Facebook’s privacy settings. Our results challenge widespread assumptions that youth do not care about and are not engaged with navigating privacy. We find that, while not universal, modifications to privacy settings have increased during a year in which Facebook’s approach to privacy was hotly contested. We also find that both frequency and type of Facebook use as well as Internet skill are correlated with making modifications to privacy settings. In contrast, we observe few gender differences in how young adults approach their Facebook privacy settings, which is notable given that gender differences exist in so many other domains online. We discuss the possible reasons for our findings and their implications.

**Faceted identity, faceted lives: social and technical issues with being yourself online** - Shelly D. Farnham and Elizabeth F. Churchill

This paper explores key issues people experience managing personal boundaries within and across social technologies. We look in particular at email and online social networks. We offer a theoretical framework for understanding the errors in assumptions about the singularity of identity that are currently inscribed into the sharing models of social technology systems. Through a questionnaire study we examine how people facet their identities and their lives, and how these facets are expressed through use of email and Facebook. We found family was an extremely important context for sharing online, and that email was still a preferred form of communication for private sharing across facets of life. Single, working men had the highest level of incompatible facets, and a higher level of facet incompatibility was correlated with increased email usage and worry about sharing in the context of social networks.

[**“I regretted the minute I pressed share”: A Qualitative Study of Regrets on Facebook**](http://www.cs.cmu.edu/~yangwan1/papers/SOUPS2011-AuthorCopy.pdf) **-** Y. Wang, S. Komanduri, P.G. Leon, G. Norcie, A. Acquisti, L.F. Cranor.

We investigate regrets associated with users’ posts on a popular social networking site. Our ﬁndings are based on a series of interviews, user diaries, and online surveys involving 569 American Facebook users. Their regrets revolved around sensitive topics, content with strong sentiment, lies, and secrets. Our research reveals several possible causes of why users make posts that they later regret: (1) they want to be perceived in favorable ways, (2) they do not think about their reason for posting or the consequences of their posts, (3) they misjudge the culture and norms within their social circles, (4) they are in a “hot” state of high emotion when posting, or under the inﬂuence of drugs or alcohol, (5) their postings are seen by an unintended audience, (6) they do not foresee how their posts could be perceived by people within their intended audience, and (7) they misunderstand or misuse the Facebook platform. Some reported incidents had serious repercussions, such as breaking up relationships or job losses. We discuss methodological considerations in studying negative experiences associated with social networking posts, as well as ways of helping users of social networking sites avoid such regrets.

S. Jones and E. O’Neil. **Feasibility of structural network clustering for group-based privacy control in social networks**. *SOUPS,* 2010.

Users of social networking sites often want to manage the sharing of information and content with different groups of people based on their differing relationships. However, grouping contacts places a significant configuration burden on the user. Automated approaches to grouping may have the potential to reduce this burden, however, their use remains largely untested. We investigate people's rationales when grouping their contacts for the purpose of controlling their privacy, finding six criteria that they commonly considered. We assess an automated approach to grouping, based on a network clustering algorithm, whose performance may be analogous to the human's use of some of these criteria. We find that the similarity between the groups created by people and those created by the algorithm is correlated with the modularity of their network. We also demonstrate that the particular clustering algorithm, SCAN, which detects hubs and outliers within a network can be beneficial for identifying contacts who are hard to group or for whom privacy preferences are inconsistent with the rest of their group. (Rebecca has read)

**I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience**

Alice E. Marwick New York University, USA, alice.marwick@nyu.edu

danah boyd Microsoft Research, USA, dmb@microsoft.com

Social media technologies collapse multiple audiences into single contexts, making it difficult for people to use the same techniques online that they do to handle multiplicity in face-to-face conversation. This article investigates how content producers navigate ‘imagined audiences’ on Twitter. We talked with participants who have different types of followings to understand their techniques, including targeting different audiences, concealing subjects, and maintaining authenticity. Some techniques of audience management resemble the practices of ‘micro-celebrity’ and personal branding, both strategic self-commodification. Our model of the networked audience assumes a many-to-many communication through which individuals conceptualize an imagined audience evoked through their tweets. (Rebecca has read – include for the notion of context collapse and why groups are important)

**Inferring Privacy Policies for Social Networking Services -** George Danezis

Social networking sites have come under criticism for their poor privacy protection track record. Yet, there is an inherent difficulty in deciding which principals should have access to user’s information or actions, without requiring them to constantly manage their privacy settings. We propose to ex- tract automatically such privacy settings, based on the pol- icy that information produced within a social context should remain in that social context, both to ensure privacy as well as maximising utility. A machine learning approach is used to extract automatically such social contexts, as well as a tentative evaluation.

**What Anyone Can Know: The Privacy Risks of Social Networking Sites** – David Rosenblum

For the Net generation, social networking sites have become the preferred forum for social interactions, from posturing and role playing to simply sounding off. However, because such forums are relatively easy to access, posted content can be reviewed by anyone with an interest in the users’ personal information.

￼

**Capturing Social Networking Privacy Preferences: Can Default Policies Help Alleviate Tradeoffs between Expressiveness and User Burden?**

Ramprasad Ravichandran, Michael Benisch, Patrick Gage Kelley, and Norman M. Sadeh

Social networking sites, such as Facebook and MySpace thrive on the exchange of personal content such as pictures and activities. These sites are discovering that people’s privacy preferences are very rich and diverse. In theory, providing users with more expressive settings to spec- ify their privacy policies would not only enable them to better articulate their preferences, but could also lead to greater user burden. In this ar- ticle, we evaluate to what extent providing users with default policies can help alleviate some of this burden. Our research is conducted in the context of location-sharing applications, where users are expected to specify conditions under which they are willing to let others see their lo- cations. We define canonical policies that attempt to abstract away user- specific elements such as a user’s default schedule, or canonical places, such as “work” and “home.” We learn a set of default policies from this data using decision-tree and clustering algorithms. We examine trade- offs between the complexity / understandability of default policies made available to users, and the accuracy with which they capture the ground truth preferences of our user population. Specifically, we present results obtained using data collected from 30 users of location-enabled phones over a period of one week. They suggest that providing users with a small number of canonical default policies to choose from can help reduce user burden when it comes to customizing the rich privacy settings they seem to require.

**Social Coding in GitHub: Transparency and Collaboration in an Open Software Repository**

Laura Dabbish, Colleen Stuart, Jason Tsay, Jim Herbsleb

Social applications on the web let users track and follow the activities of a large number of others regardless of location or affiliation. There is a potential for this transparency to radically improve collaboration and learning in complex knowledge-based activities. Based on a series of in-depth interviews with central and peripheral GitHub users, we examined the value of transparency for large-scale distributed collaborations and communities of practice. We find that people make a surprisingly rich set of social inferences from the networked activity information in GitHub, such as inferring someone else’s technical goals and vision when they edit code, or guessing which of several similar projects has the best chance of thriving in the long term. Users combine these inferences into effective strategies for coordinating work, advancing technical skills and managing their reputation.

**Internet social network communities: Risk taking, trust, and privacy concerns**

Joshua Fogel, Elham Nehmad

Individuals communicate and form relationships through Internet social networking websites such as Facebook and MySpace. We study risk taking, trust, and privacy concerns with regard to social network- ing websites among 205 college students using both reliable scales and behavior. Individuals with pro- files on social networking websites have greater risk taking attitudes than those who do not; greater risk taking attitudes exist among men than women. Facebook has a greater sense of trust than MySpace. General privacy concerns and identity information disclosure concerns are of greater concern to women than men. Greater percentages of men than women display their phone numbers and home addresses on social networking websites. Social networking websites should inform potential users that risk taking and privacy concerns are potentially relevant and important concerns before individuals sign-up and create social networking websites.

**College students' social networking experiences on Facebook**

Tiffany A. Pempek, Yevdokiya A. Yermolayeva, Sandra L. Calvert

Millions of contemporary young adults use social networking sites. However, little is known about how much, why, and how they use these sites. In this study, 92 undergraduates completed a diary-like measure each day for a week, reporting daily time use and responding to an activities checklist to assess their use of the popular social networking site, Facebook. At the end of the week, they also completed a follow-up survey. Results indicated that students use Facebook approximately 30 min throughout the day as part of their daily routine. Students communicated on Facebook using a one-to-many style, in which they were the creators disseminating content to their friends. Even so, they spent more time observing content on Facebook than actually posting content. Facebook was used most often for social interaction, primarily with friends with whom the students had a pre-established relationship offline. In addition to classic identity markers of emerging adulthood, such as religion, political ideology, and work, young adults also used media preferences to express their identity. Implications of social networking site use for the development of identity and peer relationships are discussed.

**xBook: Redesigning Privacy Control in Social Networking Platforms**

*Kapil Singh, Sumeer Bhola, Wenke Lee*

Social networking websites have recently evolved from being service providers to platforms for running third party applications. Users have typically trusted the social networking sites with personal data, and assume that their privacy preferences are correctly enforced. However, they are now being asked to trust each third-party application they use in a similar manner. This has left the users’ private information vulnerable to accidental or malicious leaks by these applications.

In this work, we present a novel framework for building privacy-preserving social networking applications that retains the functionality offered by the current social net- works. We use information flow models to control what untrusted applications can do with the information they receive. We show the viability of our design by means of a platform prototype. The usability of the platform is further evaluated by developing sample applications using the platform APIs. We also discuss both security and non- security challenges in designing and implementing such a framework.