Susceptibility to Social Influence of Privacy Behaviors: Peer versus Authoritative Sources

Tamir Mendel
Department of Industrial Engineering, Tel Aviv University
Tel Aviv, Israel
tamirmendel@tau.ac.il

Eran Toch
Department of Industrial Engineering, Tel Aviv University
Tel Aviv, Israel
erant@tau.ac.il

ABSTRACT

Privacy in Online Social Networks (OSNs) is a dynamic concept, contingent on changes in technology and usage norms. Social influence is a major avenue for adopting online behaviors in general and privacy practices in particular. In this study, we examine how the source of influence affects the perceived behavioral intention to adopt privacy behavior. Our findings are based on a randomized experiment (167 U.S.-based Amazon Mechanical Turk workers) using a custom Facebook application that collects feedback from participants regarding their intention to adopt privacy practices from different types of sources, including authoritative organizations and friends with varying tie strength correlative. Our results show that the source of social influence affects the susceptibility to adopt certain privacy behaviors and that there are different patterns of influence for security and privacy norms. More interestingly, susceptibility is modulated by the privacy perceptions of the user: users with high perceived behavioral control are more susceptible to peer influence. Additionally, we show that the intention to adopt privacy practices is correlated with the intention to further influence other people.

Author Keywords

Privacy; online social networks; social influence; authoritative influence; peer influence; behavioral intentions.

ACM Classification Keywords

H.5.2. Information interfaces and presentation (e.g., HCI): Miscellaneous

INTRODUCTION

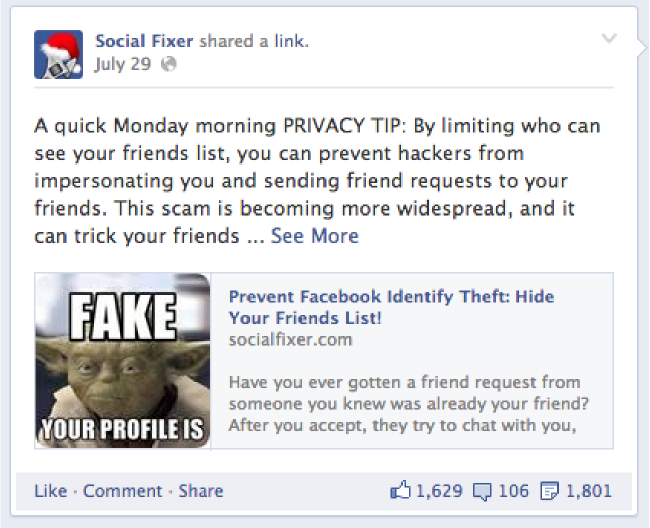
As the reach of online social networks (OSNs) expands, so do people's privacy concerns. Recent surveys have shown that Americans' privacy concerns regarding social networks have increased in recent years [37]. Several studies have shown that users often regret posting information on social media due to privacy harm [51] and that managing privacy in OSNs is often a difficult task for users due to the complicated mental model of privacy settings [38]. However, in recent years, we have witnessed the dynamic nature of the norms surrounding social networking privacy usage. Several studies point to a gradual and ongoing awareness of privacy among users, with Facebook users becoming more active in managing their accounts, pruning friends and updating their privacy settings [36], and becoming increasingly less likely to share their profile elements in public [48, 19]. These phenomena point to the potential of changing norms to incite change and raise awareness regarding privacy.

Recent works suggest that social influence is a promising approach to inciting normative change. Studies have shown that a wide set of behaviors are contingent upon social influence in social networks, including the spread of obesity [14], quitting smoking [15], adoption of online entertainment products [3], reduction of household energy consumption [44], and sensitivity to Facebook's security features [17]. Presenting social clues, such as showing the number of friends who adopted a feature, has been shown to increase the adoption rates of security features on Facebook [18] and the awareness of informed privacy consent [7].

There are several indicators that demonstrate how social network users exchange and share information about privacy. Lewis et al. [35] show that having a roommate with a private profile is a strong predictor for having a private profile. Also, information about privacy is exchanged through the social network itself [34], and user interfaces that inform users about their friends' privacy choices [41]. While we can see many examples of privacy information exchange in action, such as the viral posts displayed in Figure 1 and shared 1,801 times, it is still unclear how the influence is carried, and what is the effect of different channels of influence. Existing theories and methodologies could fall short in understanding social influence of privacy behavior. Privacy is a normatively charged subject, with people's attitudes towards privacy in online social networks varying between unconcerned to fundamentalists [29, 13]. Unlike the case of security, in which the threat is external (expressed in most cases by the alienating term "hackers"), for privacy, the adversarial model is more complex and depends, among other variables, on the user's approach to personal information.

It is unclear whether social influence can serve as an effective tool to drive the adoption of privacy practices. It might be the case that privacy may be similar to political behavior, which does not obey straightforward diffusion patterns but is

CSCW 2017, February 25–March 1, 2017, Portland, OR, USA.
Copyright © 2017 ACM ISBN 978-1-4503-4189-9/16/10 ...$15.00.
http://dx.doi.org/10.1145/2998181.2998323



Social Fixer shared a link.
July 29

A quick Monday morning PRIVACY TIP: By limiting who can see your friends list, you can prevent hackers from impersonating you and sending friend requests to your friends. This scam is becoming more widespread, and it can trick your friends ... See More

Prevent Facebook Identify Theft: Hide Your Friends List!
socialfixer.com

Have you ever gotten a friend request from someone you knew was already your friend? After you accept, they try to chat with you,

Figure 1. An example of an actual viral post that contains a privacy tip: a suggestion to hide the user's friends list.

dependent on how users' attitudes affect adoption patterns [8, 43]. The source of social influence can be significant as well because of prevalent mistrust regarding the role of privacy in social networking platforms [22, 13] and may be less susceptible to influence that originates from the social network operator. As a result, users might resist and distrust nudging mechanisms that aim to push users towards more privacy-oriented behavior (e.g., [50]).

Therefore, we ask to understand the effect of sources of influence and users' own attitudes on susceptibility to adopt privacy behavior. We base our model on the Theory of Planned Behavior (TPB) [2], a well-established framework for users' decision-making in the context of persuasion in social networks [9, 16]. We conduct an experiment in which we measured users' intention to adopt and to share privacy practices while we manipulate the sender (strong-tie social relations, weak-tie social relations and authoritative entities) and the content of the message (security versus privacy). We correlate the behavioral intention with user's privacy concerns and perceived privacy control to understand the interaction between users' privacy attitudes and the manipulations. 167 American Amazon Mechanical Turk workers had participated at the experiment.

Our results contain three main findings. First, perceived privacy control mediates between the sender category and the behavioral intention. Second, users intend to adopt privacy practices when the privacy concern is high or PBC is high. Finally, users who intend to adopt privacy behaviors are more likely to promote the behavior by intending to share the practice with their social network. These results are useful in understanding how social network users learn from each other and from organizations regarding privacy practices, as well as the role social network has in constructing privacy behavior. Furthermore, our work can facilitate designing systems that aim to induce changes in users' norms, such as systems that can dynamically allocate the right sender, and designing the right post to influence a user's behavior.

BACKGROUND AND RESEARCH MODEL

The background to this work relies on three theoretical fields: influence in social networks, privacy in social networks, and planned behavior. We finalize this section by presenting our research model and hypotheses.

Social Influence

Researchers from psychology, sociology, and economics study how peers can influence behaviors, norms, and preferences in social networks. Christakis and Fowler observed that health behaviors are contentious in offline social networks, including life-threatening behaviors, such as obesity [14], and life-saving behaviors, such as quitting smoking [15]. Similar dynamics have also been reported for peer-based recommendation networks in electronic commerce [40] and for adopting products through online social networks [3].

Campaigns based on normative messages with social proofs have been shown to incite behavioral changes, such as reducing household energy consumption [44], influencing retirement saving behavior [28], increasing sensitivity to Facebook's security features [17], increasing the adoption rates of security features on Facebook [18], and increasing the awareness of informed privacy consent [7]. We observe that there is similarity in the influence between health behaviors and privacy behavior. For example, many agencies promote cyber security "hygiene", emphasizing how human behavior can improve individual and group cyber security and privacy [42].

Social Network Privacy

Privacy in OSNs is an inherently contested issue [1], and users exhibit varying attitudes towards the importance of privacy. We know that similar contested issues, such as political views, do not obey contagion patterns on social networks due to their polarizing nature [8, 43, 10]. Additionally, it is unclear how users will react to future promotions by organizations, which are now widespread in social media through Facebook "Pages" (on Facebook) or organizational accounts on Twitter and LinkedIn.

We follow the distinction made by Dourish and Anderson [21] and others between privacy and security in people's collective practices. In the context of social networks, security relates to the way people's systems and information are vulnerable to external attacks from outside the system. Privacy, on the other hand, relates primarily to the way people might lose control over their information to other peers of the system (i.e., other users) or to the system itself (e.g., Facebook). The discourse around security practices revolves around securing the user's account from hackers [52], while the discourse around privacy practices revolves around the way individuals might lose control over their information, losing their confidently and autonomy when other people gain access to confidential information or the network operators use information for advertising or other unsolicited ways [27, 48].

The distinction between security and privacy may have implications to the collective practices that surround them and to the way to promote certain practices. Unlike security, in which the adversary is external to the system, in privacy, there is an inherent conflict between the user and the system [21, 38]. Because many individuals mistrust the way social networking platforms approach privacy [22, 13], having those organizations take part in influencing users may cause a boomerang effect, pushing users away from privacy-awareness. Therefore, we cannot assume that privacy is comparable with less disputed issues, such as security or even power consumption. This observation raises several question regarding strategies to promote privacy and to impact the way collective privacy behaviours can be influenced. It might be the case that existing social influence models, such as [26, 3, 18] should be altered to address privacy behaviors.

Social Influence and Intentions

The channel of social influence refers to the medium through which influence is communicated or transmitted. Granovetter suggests that in social networks, ”*most of the influence is carried through strong ties*” [26], and strong ties are instrumental for influencing both online and real-world behavior [10, 4]. Aral and Walker [3] showed that susceptibility to influence determines how people adopt and promote certain behaviors and that social relations with stronger ties and with a larger number of mutual friends are significantly more influential. However, due to the contested nature of privacy, it is unclear whether these theories can be extended to privacy.

To investigate privacy social influence, we ask regarding the effect of the influence channel (the sender of an influential message) on the susceptibility of users to adopting a privacy practice and how the behavior is likely to continue to spread through the network. To measure the impact of influence, we rely on the Theory of Planned Behavior (TPB) [2], which is the most proximal determinant of behavior. According to the theory, intention is influenced by three constructs: attitudes, i.e., an individual’s positive or negative evaluation of performing a behavior, subjective norms, i.e., an individual’s perceived social pressure to perform the behavior, and perceived behavioral control, i.e., an individual’s perception of control over performing the behavior. According to Azjen, given two individuals with the same level of intention to engage in a behavior, the one with more confidence in his or her abilities is more likely to succeed than the one who has doubts.

The Theory of Planned Behavior (TBP) has been used as a prediction model of various behaviors related to trustworthiness and privacy in Internet purchasing behavior [24] and OSN usage characteristics [9, 16]. A meta-analysis showed that, on average, the model accounted for 39 percent and 27 percent of the variance in intention and behavior, respectively [5].

Hypotheses

This study examines the social influence of different privacy influence channels by applying an extended TPB model to adoption of privacy behaviors in OSNs. The behavior in question is adopting the privacy behavior suggested by a sender. We hypothesize that personal senders are more influential in promoting privacy behaviors than authoritative senders (hypothesis 1) and that strong ties are more influential than weak ties (hypothesis 2). Based on the varying personal abilities in managing privacy, processing the information, and carrying out an advise, we predict that higher *Perceived Behavioral Control (PBC)*, which reflects the self-efficacy of using privacy settings [38], will be associated with different behavioral intentions to adopt privacy behavior from different channels (hypothesis 3). Finally, we hypothesize that higher behavioral intention is positively associated with a higher willingness to promote privacy behavior (hypothesis 4).

METHOD

Study Design

The study was based on an experimental design, as can be seen in Figure 2, manipulating the sender category (between subjects) and the content of messages (within subjects). The end-result is a split-plot design in which participants were placed within one sender category group for the whole duration of the experiment, with repeated measures for 6 randomized messages.

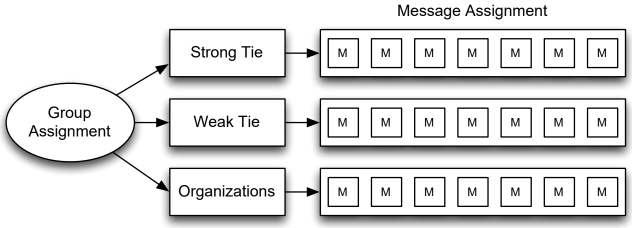


Figure 2. The design of the experiment, including assignment of participants to groups (between subjects) and assignment of messages to each participant (within subject).

The study was based on a simulation of influential messages from the participants’ actual Facebook social network relations, to maintain the validity of the intention measurement. We developed a custom Facebook application to analyze the participants’ Facebook networks in real time, differentiated between strong tie and weak tie contacts, and simulated an influencing message from real Facebook contacts. The study apparatus contained a displayed message from a simulated sender and a questionnaire. The message questionnaire, in which each participant was asked to refer to the simulated sender and message, was presented below the post (see Appendix A.1). Participants repeated this questionnaire six times for six randomized messages out of a pool of , each trial with different content according to the sender group that was randomly assigned to them. At the end of the experiment, participants responded to an exit questionnaire (see Appendix A.2). The study received the approval of the institutional ethics committee.

Independent Variables

The influence channel was defined through the *sender category*, which represents the type of entity that sends the information to the user. The three conditions included at the experiments were authoritative organizations, strong tie contacts, and weak tie contacts. We selected authoritative organizations that are often involved in the discourse of privacy, including Facebook itself, media organizations, the government, and non-profit organizations. The full list of authoritative senders is described in Table 1. We refer to these types of senders as the "organization" category.

Table 1. A list of authoritative senders in the organization category

Type	Sender
Facebook	Facebook Tips Page, Facebook and Privacy Page
Media	CNN Page, NBC Page
Government	USA.gov, OnGuardOnline.gov
Nonprofit	Family Online Safety Institute, iKeepSafe Coalition, Insafe

We correlate tie strength based on two predictive measures: intimacy and intensity. Based on the work of Gilbert and Karahalios [25], we calculate the estimated tie strength based on the communications between the participant and people from her social network. It is important to emphesize that our value is not correlated fully with tie strength, but it was found to be a strong predictor to it in the context of communication and interaction on Facebook [25]. Definition describes the prediction of tie strength between a given user (i) and a given Facebook friend (j), summing three parameters: number of messages between the user and the friend (I$_{fi,u}$); number of likes by the friend regarding the user's posts (L$_{fi,u}$); number of the friend's comments on the user's posts (C$_{fi,u}$).

Definition 1. Predicted tie strength measure between user i and j

$$TS_{i,j} = W_I \frac{(I_{f_i,u} + I_{u,f_i})}{\max_j\left(I_{f_j,u} + I_{u,f_j}\right)} + W_L \frac{L_{f_i,u}}{\max_j\left(I_{f_j,u}\right)}$$

$$+W_C \frac{C_{f_i,u}}{\max_j\left(C_{f_j,u}\right)}$$

Each parameter is normalized by the maximal user's Facebook friend value. It can be ranked between different contacts, which belong to the same user; the higher the tie strength, the closer friend the contact is. A contact is classified as a strong-tie under two conditions: the strength measure is higher than zero and the measure is at the top 15% of ranking friends. The weights W_I, W_L, and W_C were determined using the regression reported by Gilbert and Karahalios [25].

The content of the message was chosen to include a variety of messages that reflect actual privacy advice propagated through Facebook. Overall there were 8 privacy messages and 3 security messages, which were randomized for each post. The content was taken from two popular Facebook pages that guide users in the management of privacy and security: "Facebook and Privacy"[1] (2,600,000 likes) and "Social Fixer"[2] (330,000 likes). The full list of messages is displayed in Appendix A3, but to illustrate the messages, the following is an example of one of the messages from the Facebook and Privacy page:

> "*Control your audience. Whenever you share something on Facebook, you can choose who sees it. You'll find our audience selector tool when you share status updates, photos, videos and other stuff. Just click the tool and select the audience with which you want to share.*"

The content included several aspect of privacy management. Following the definitions by Dourish and Anderson [21], we aimed for the majority of messages to address privacy, rather than security. The majority of messages were aimed to help users controlling private information from other social network users in various levels of closeness, directly by sharing the information or indirectly through mechanisms such as advertising. We focused mainly on these activities because we know that they are the most pressing to social network users [47]. Also, these are the activities in which there is an ongoing increase in recent years, point most commonly used [48]. We also included a small number of posts that help users secure themselves against external attacks, to test whether the content had an impact on the answers.

Planned Behavior Variables

Following Francis et al. [23], *behavioral intention* was evaluated using three questions: expectation to follow, desire to follow, and intention to follow (questions 2, 3, and 6 in Appendix A.1). All items were scored using a 5-point Likert scale. We also asked two questions about the willingness to share or like the post with the participant's social network (questions 5 and 7 in Appendix A.1; e.g., "I am willing to share the suggested advice with my friends"). Furthermore, we asked participants about their willingness to share and "like" the post, two actions that result in possible exposure of the post to their social network.

The users' *attitudes* were chosen to reflect privacy access concerns, based on Stutzman's questionnaire [46], measuring different aspects of concern using a 9-item validated questionnaire by that measures OSN access concerns (e.g., "I am OK with friends accessing my Facebook timeline" and "I am concerned with the consequences of sharing identity information"). *Subjective norm* was measured using two items (questions 23c and 23d in Appendix A.2; e.g., "My friends on Facebook don't care about their online privacy"). The perceived behavioral control (**PBC**) is based on a measure by Madejski et al. [38] for self-efficacy of using privacy settings (questions 23a and 23b in Appendix A.2; e.g., "I know how to change the privacy setting on my Facebook account"). Due to low scale reliability, only the highest loading item reflecting the self-efficacy component of PBC was used to measure PBC (question 23b).

Control Variables

To control for personal attitudes of participants, we have measured several attitudinal variables. For each post, we measured the *trust* Other measures included an item that measured the trust users have toward the sender (i.e., "I do not

[1] A Facebook group operated by Facebook inc. that promotes privacy and security information: https://www.facebook.com/fbprivacy

[2] An independent Facebook group that dispenses information and tools to help users manage their privacy and security https://www.facebook.com/socialfixer/

Table 2. Participants demographics divided by between-subject study condition

Property	Conditions		
	Strong tie	Weak tie	Organizations
Participants	52	45	70
Mean posts (s.e)	140.52 (11.43)	144.33 (13.74)	163.37 (10.14)
Age 18-24	23 (45%)	10 (22%)	23 (33%)
Age 25-34	21 (40%)	23 (51%)	28 (40%)
Age 35+	8 (15%)	12 (27%)	19 (27%)
Females	31 (60%)	33 (73%)	44 (63%)
Males	21 (40%)	12 (27%)	26 (37%)

trust the person or entity that published the post.”). Also, we had measured the perceived ability to act upon the advice (i.e., “I do not know how to implement the advice suggested using Facebook’s setting.”)

To control for participants’ actual privacy behaviors, each participant’s *privacy agility* was measured, which measures how often the participant switches between different audiences in consecutive posts, reflecting the privacy practice and awareness of the participant. Privacy agility was calculated as the entropy of privacy decisions according to Equation 2, where (P_u) is the categories of the audience of post *i* (public, friends-of-friends, friends, custom, only-me). X_i is set to 1 if the user shared audience in post i-1 is different from that in post i; otherwise, it is set to 0.

Definition 2. Privacy agility calculated for user u

$$agility_u = \log\left(\frac{\sum_{i \in P_u}(x_i) + 1}{|P_u|}\right)$$

Also, we have analyzed the number of friends for each participant, which was not normalized, and the number of posts. Finally, at the exit questionnaire, participants indicated their age, gender, education, years of Facebook usage, average daily time spent on Facebook, number of published posts, friends interacted with on Facebook, and reasons for using Facebook. As age, gender, education, number of friends, and number of posts were all found to affect privacy behavior [31, 20], we have added those variables to the analysis.

Participants

We recruited participants via Amazon Mechanical Turk (MTurk), a crowdsourcing tool that is commonly used in OSN and in privacy research (e.g., [51, 49]). American MTurk workers, who were the population of our study, have similar amount of personal information online as the general American population, and have higher levels of awareness of privacy threats than the general population [30]. The participants were required to be at least 18 years old and were American Facebook users, to control for language and regulatory framework. The participants were exposed to the fact that the study’s objective is about privacy and social influence. The minimal sample size for each condition was set to 42, using a power analysis, in which we designed for an ANOVA analysis with 3 groups, medium effect size (0.25), significance levels of 0.05, and power of 0.7.

We had removed several participants that did not have enough friends for analysis of tie strength, there were more participants in the organization condition than in the other conditions (as can be seen in Table 2). Furthermore, some of the participants left the experiment at the beginning; the percentage leaving the tie strength condition was 20% and organization condition was 10%. Therefore, we conducted a Kruskal Wallis non-parametric test of independent samples showing that there is no significant effect of sender categories on the privacy concern, PBC, privacy access concern, and number of posts, i.e. the difference of participants leaving between tie strength and organization did not affect the control variables. At the end, we had 167 participants, 108 females and 59 male.

Preprocessing and Data Analysis

The first step of the preprocessing stage was to clean the data in iteration level. First, to counter learning and fatigue effect, the first and last trails were removed from the dataset [32]. Second, to ensure participant seriousness, we have checked if the distances between different behavioral intention variables are higher than three, and if so, the record was removed. The checkup was according the intention group’s questions: exception to follow, desire to follow, and intention to follow. The purpose of this check was to ensure that participants read and understood the questions beneath the post. After the cleanup stage, we had 167 valid participants out of the original 172.

We calculated Cronbach’s Alpha for the privacy access concern questionnaire and therefore we divided the questionnaire into two parts according to the alpha measures: 0.78 and 0.68, respectively. Thus, we continued with the average value that has higherinternal consistency. Additionally, the Cronbach’s Alpha of the behavioral intention variables is 0.92, exhibiting very high internal consistency.

Because each respondent provided data on several messages, we used Linear Mixed Effects (LME) regression to account for the unbalanced selection of messages (even though they were randomized), to control for repeated measures originating from the content of promotional messages [6]. LME allows us to control the dependence between observations, where the null hypothesis contains the nave independent variable, which are the demographics. The model hypothesis contains the other independent variable. P-values were obtained by likelihood ratio tests of the full model hypothesis against the null hypothesis. For each model, we have calculated the variance explained (The R^2 value) for both the marginal and conditional effects, representing variance explained by fixed factors and with variance explained by both fixed and random factors, respectively [39].

RESULTS

In the following sub-sections, we explain the results, starting with descriptive statistics, effects of the independent variables on behavioral intentions and promotion.

Descriptive analysis

Figure 3 shows the number of the participants in each privacy access concerns value. It can be seen that only 7% of the participants have privacy access concerns higher than four. It means that most of participants still allow some access to their

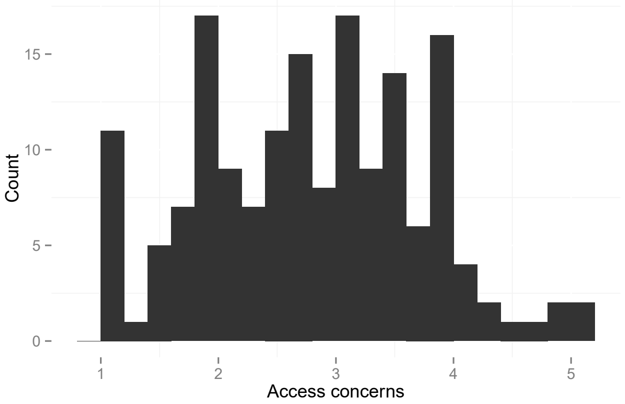


Figure 3. Frequency of mean privacy access concerns

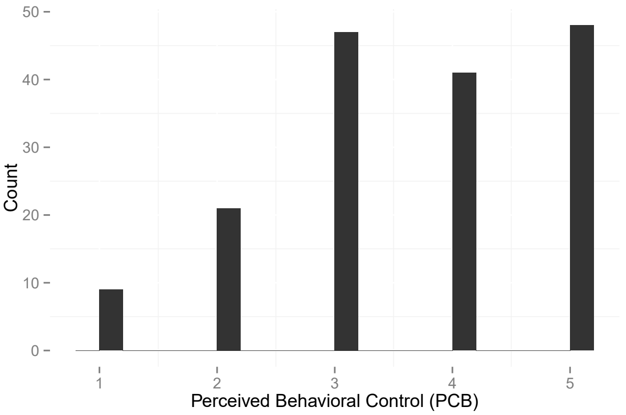


Figure 4. Frequency of PBC

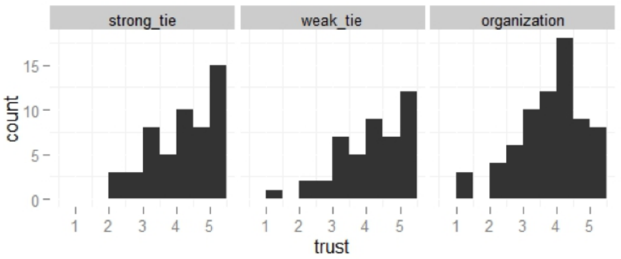


Figure 5. Frequncy of trust. There is a statistical significant difference between strong tie and organization

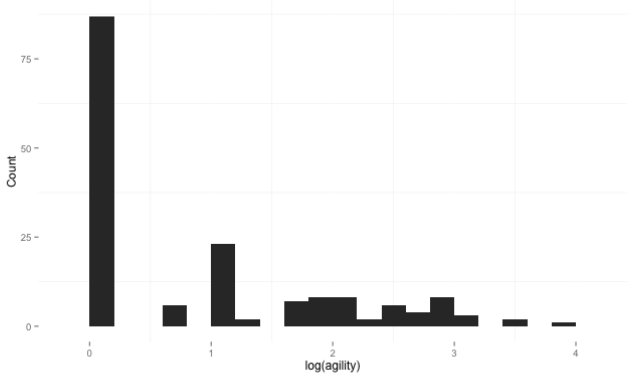


Figure 6. Frequency of agility

Facebook data. Figure 4 displays the frequency of PBC. Only 30% of participants have full behavioral control. The privacy agility is presented in Figure 6. The mean value for agility is 0.21 and the standard deviation is 0.28. 52% of participants using only one audience when sharing the post. This means that most of the participants use the default privacy option, when sharing a post. We had asked the participants to review their trust to the sender of each of the posts. The frequency of their responses is displayed in Figure 5. The average trust is 3.8, with high variance of 1.26. The average trust for a person is about 10% higher than the trust for an organization (Wilcoxon rank sum test, $p < 0.05$). However, there is no statistically significant difference between weak-tie and strong-tie connections.

Effects on Behavioral Intentions

A hierarchical multiple linear mixed effect analysis was conducted to predict intention to adopt privacy behavior (Table 3). In step 1, we modeled demographic variables that include age, gender, education, average number of weekly posts, and number of friends. This model significantly accounted for 13 percent of the variance in intention (AIC=1619.6, BIC=1713.8, DF=512, p<0.01). At step 2, the TPB variables, attitude (access concerns), subjective norm, and PBC, significantly increased the proportion of variance to about 24% percent (AIC=1615, BIC=1743.4, DF=503, p<0.01, p<0.01). The final model provides a good fit for data, accounting for 28 percent of the fixed effects variance and, of the significant predictors, the content of the message, the condition, trust, agility and the interaction between PBC and the condition (AIC=1569.5, BIC=1736.4, DF=494, p<0.01). The final model without the demographics fits the data with marginal R^2 of 0.17 and a conditional R^2 of 0.59 (AIC=2461.4, BIC=2545.9, DF=494, p<0.01).

Overall, the behavioral intention for both weak and strong ties was significantly higher than organizations (coefficient of $-1.17, t = -2.1, p < 0.02$). Surprisingly, the behavioral intention for strong ties was lower than of weak ties (coefficient of $-1.61, t = -2.9, p < 0.03$). The condition for strong tie is not displayed in table 3, because it is the first condition and is absorbed in the intercept. PBC mediates the effect of the sender category on behavioral intentions. As visualized in Figure 7, participants with low PCB are affected more by persons than organizations (Wilcoxon rank sum, $x^2 = 744.5, p < 0.05$). When PBC is low, users tend to be influenced by their contacts. When PBC is higher, the effect of all influence channels is similar. To understand this result, we may look at trust, which has a very strong positive effect on behavioral intention (coefficient of 0.24, $t = 2.192, p < 0.02$). As Figure 8 shows, participants with

Table 3. LME fixed effects coefficients and significance of the behavioral intention. The strong tie category is inside the intercept; thereby, it does not appear as an independent fixed effect coefficient. Significant p-value codes: . $p < 0.1$; * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$.

Property	**Step 1**		**Step 2**		**Step 3**	
	Estimate	Std. Error	Estimate	Std. Error	Estimate	Std. Error
(Intercept)	**3.05*** **	**(0.46)**	0.55	(0.15)	0.10	(0.67)
Age 25-34	**0.34***	**(0.17)**	0.24	**(0.17)**	**0.28.**	**(0.15)**
Age 35+	0.38.	(0.20)	0.23	(0.18)	0.31.	(0.19)
Gender: male	**-0.51*** **	**(0.15)**	**-0.42** **	**(0.14)**	**-0.42***	**(0.13)**
Education: no high school	0.55	(0.61)	0.32	(0.54)	0.34	(0.22)
Education: high school	**0.60***	**(0.25)**	0.41.	(0.22)	-1.05	(0.78)
Education: professorial degree	-0.16	(0.76)	-0.30	(0.67)	-0.37	(0.65)
Education: undergraduate degree	0.17	(0.17)	0.23	(0.15)	0.24	(0.14)
Education: graduate degree	**-1.81***	**(0.85)**	-1.23	(0.86)	-1.17	(0.76)
Income	0.05	(0.04)	0.07	(0.04)	0.04	(0.04)
Number of posts	0.0008	(0.001)	0.0008	(0.001)	0	(0)
Number of friends	**0.0006***	**(0.0002)**	**0.0006***	**(0.0002)**	0	(0.14)
PBC			-0.0057	0.057	0.15.	(0.09)
Subjective norm			0.11	(0.1)	0.04	(0.06)
Attitudes: strong ties			0.30.	(0.18)	0.30	(0.18)
Attitudes: weak ties			0.36.	0.18	**0.39***	**(0.19)**
Attitudes: family			**-0.30***	**(0.14)**	**-0.31***	**(0.14)**
Attitudes: strangers			-0.05.	(0.09)	-0.07	(0.09)
Attitudes: colleagues			-0.18	(0.13)	-0.19	(0.13)
Attitudes: sharing			-0.11.	(0.06)	-0.08	(0.07)
Attitudes: identity			**0.19***	**(0.08)**	**0.17**	**(0.08)**
Agility			**0.15***	**(0.06)**	**0.14***	**(0.06)**
Trust			**0.22*** **	**(0.03)**	**0.23*** **	**(0.03)**
Condition: organization					**-1.17***	**(0.54)**
Condition: strong ties					**-1.61** **	**(0.54)**
PBC * organization					**0.29***	**(0.13)**
PBC * strong ties					**0.43***	**(0.14)**
Marginal R^2	**0.130**		**0.260**		**0.281**	
Conditional R^2	**0.45**		**0.47**		**0.493**	

low PCB were less trustful of organizations then users with high PBC. The actual privacy behavior of participants can also serve as a predictor for their behavioral intention. Participants with high privacy agility had a higher change to adopt the behavior (coefficient of 0.14, $t = 2.241, p < 0.05$).

PBC has a positive effect, but only in an interaction with the sender category. Users who felt that they have the capabilities of carrying out privacy decisions were more apt to adopt new privacy behaviors. On the other hand, subjective norm was not a significant predictor for behavioral intention. The effect of attitudes was mixed. Higher concerns for access by weak ties connections have a significant positive effect on behavioral intentions (coefficient of 0.18, t=2.814, p=0.005) while concerns regarding family (coefficient of -0.35, t=-2.38, p<0.01) and colleagues (coefficient of -0.32, t=-2.328, p<0.02) have a negative effect. A possible explanation is that content of most of the messages was more suitable to protect privacy against unsolicited access from weak tie connections and strangers.

We model the impact of different organization types through LME analysis, producing a model with an R^2 of 0.274 (x^2= 91.802 p<0.001). When the PBC is high, there is a similarity between Facebook and all organizations. However, when the PBC is equal to or lower than the median (three), users are less likely to adopt a behavior suggested by Facebook than by other oranizations.

Promotion of Privacy Behavior

We measure behavioral promotion according to a participant's self-reported willingness to share or like a post, i.e., behaviors that expose a post to a user's social network. LME analysis was used to analyze the relationship between the intention to share or like and the behavioral intention. The marginal R^2 for liking intention is 0.307 (x^2=220.76, p<0.001) and for sharing intention is 0.321 (x^2= 222.45,

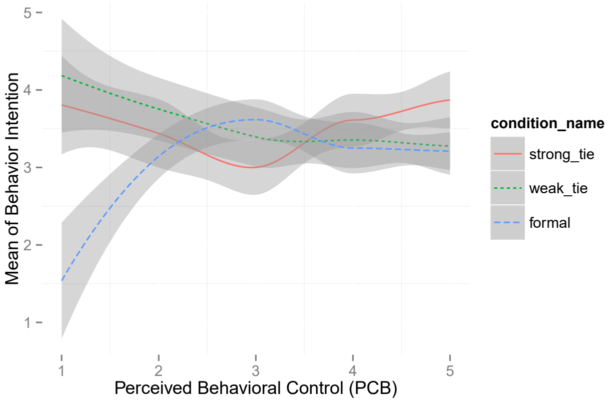


Figure 7. Behavioral intentions according to sender categories and PBC

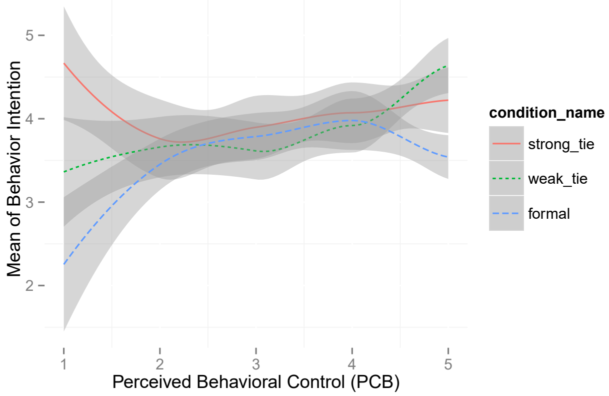


Figure 8. Trust intentions according to sender categories and PBC

p<0.01). Figure 9 provides a visual depiction of the linear regression of liking and sharing, demonstrating similarities in the way the two promotional behaviors are related to behavioral intention. There is also a positive correlation between the relevancy of a post, i.e., privacy behavioral intention (r=0.72; p¡0.0001), like (r=0.59; p¡0.0001) and share (r=0.54; p¡0.0001). Because we did not control behavioral intentions, these results are correlative in nature rather than pointing to causality.

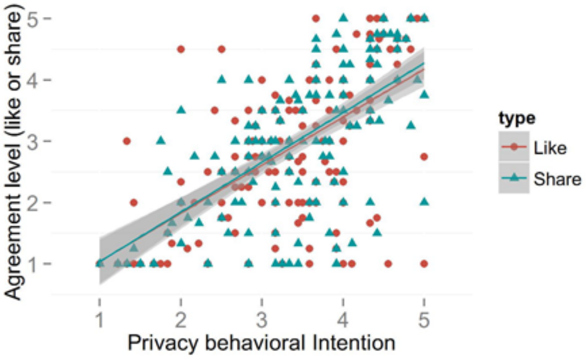


Figure 9. Correlation between mean of participant's willingness to 'Like' vs. Behavioral Intention

DISCUSSION

The present study examined the application of an extended TPB to measure the susceptibility to social influence of privacy behaviors. The finding provide support for hypothesis 1, people are more influential than organizations. However, hypothesis 2 was not supported, as weak ties were more influential than strong ties. The way ties were calculated may have led to a smaller number of possible contacts, with whom the participant may not address as a good source for privacy. Interestingly, people are more influenced by other people when their ability to manage privacy is low (hypotheses 3). Because privacy is related to people's trust of authority and large organizations, such as Facebook [29], those with lower privacy efficacy might be less trustful of these organizations and hence less willing to accept their influence. This notion is further strengthened by the positive correlation between trust and behavioral intention.

Our findings demonstrate the contexts in which social network users learn from their friends about privacy practices. Extending existing works [35], we can see that privacy access concerns and PBC have positive effects on the participants' willingness to adopt privacy behaviors. We also see that privacy agility has a positive effect on susceptibility to privacy influence. Because privacy agility is an observed rather than self-reported variable, representing the rate of changes in privacy settings, the result can be used to identify susceptible users automatically. This may mean that participants who are more active in managing their privacy settings can be more open to receiving knowledge regarding privacy practices.

Individuals with higher behavioral intention have higher willingness to promote the behavior, supporting hypothesis 5. These results strengthen previous results by Das et al. [17] but contextualize them in the field of privacy. This result allows us to estimate the proportion of users that will adopt a privacy behavior before promoting it. This finding connects two theories: behavior adoption and information diffusion models. This means that by measuring the promotion of a behavior, we may be able to measure the adoption of the behavior. Of course, our findings are based on a self-reported questionnaire regarding behavioral intention and are therefore limited in predicting actual behavior.

We see some demographic differences that impact the susceptibility to influence. Young adults (aged 25-34) were more susceptible than other groups, and men were less susceptible than women. The last result add another dimension to previous works, by Lewis et al. [35] and boyd and Hargittai [11], which show that women are more attuned to privacy in online social networks. Surprisingly, educated participants were less susceptible to privacy influence.

Our results demonstrate that the contingency of privacy behavior is dependent upon people's attitudes. Therefore, theories that explain behavioral and knowledge diffusion [3, 18, 12, 43] may not be applicable to privacy behaviors. Our findings demonstrate that privacy requires different strategies of approaching users rather than one monolithic one. Another theoretical contribution is to the field of social influence itself. To the best of our knowledge, this is the first paper that compares social influence by organizations versus social influence by people. In contemporary social networks, organizations (e.g., Facebook Pages or corporate Twitter accounts) live side by side with humans, creating a completely new landscape for social interaction and social influence. Our results show that patterns of trust and self-efficacy are the determinants in differentiation people make between organizations and people. It is important to put an emphasis, at this point, about the special context of privacy. It might be the case that in less contested fields, we would not see differences between organizations and people.

Our findings have several implications to privacy design and practice. Social network designers and operators can use these results to better design tools to influence users' privacy. One immediate conclusion is that multiple channels of influence are needed to address different types of populations, each with its own patterns of efficacy and trust. For example, it may be advisable to share some information formally, and some of it through viral distribution. At the same time, the ability of sophisticated influence tool creators raise some alarm. The fact that it is possible to effectively change people's behavior through personalized influance channel may raise concerns among many users. We argue that individuals can use the findings of this study to be more aware of the way they may be manipulated, and to take into account this new knowledge when being exposed to viral or authoritative communication.

The findings of this paper raise the question of how norms develop in response to the architecture of the system. Lessig's framework of cycberspace regulation points to an interaction between the architecture of the social network and the norms that govern the way people use the architecture (the [33]. Our findings show how both the system operators and the people using the systems can incite normative change, but behavioral change can be faster and more powerful if users are convinced to influence each other. To incite changes in the norms, systems can dynamically find the right path needed to influence user behavior, deciding, for example, whether to directly send normative messages. While the study was carried out in the domain of privacy, our methodology can be extended to other domains. For example, a company that wants to influence people to purchase a certain product may use our methodology to understand the appropriate communication channel to contact the potential buyer more effectively, i.e., directly or through other members of their social network.

Limitations and Future Work

In our study, potential participants were requested to authorize a Facebook application to participate at the study. Therefore, there might be some self-selection process, in which participants were notified about the invasive data collection process but chose to participate in the study nevertheless. In the paper, we rely on the experimental arrangement to counter the selection biased, measuring similar levels of PBC in all the conditions, and controlling for PBC and privacy sensitivity in the regression. We also compared the Facebook privacy settings of the study population with data surveyed from the general population by Pew [36], and found similar distributions of usage of different privacy options.

The experiment is based on asking participants for their reactions on hypothetical posts in hypothetical social context (but with real Facebook friends). While behavioral intention questionnaires were found to be correlative with actual behaviors [45], we do not know of a validation of this relation in OSNs privacy scenarios. An interesting followup work could be to confirm and understand this relation. To partially compensate for the gap between manifested intentions and behavior, it is important to note that our questionnaire included questions about liking and sharing the post, two relatively straightforward actions, which were highly correlated with the behavioral intentions.

CONCLUSIONS

Through an experimental approach, we showed the potential and unique properties of social influence on privacy behavior. Social influence can drive privacy awareness and behavior and can urge users to adopt privacy features and share them with others. We started the work by asking whether the source of the influence, organizations versus people and people with varying levels of tie strength. Our results indicate that content matters: influence of privacy messages is inherently different than that of security messages. Users are more susceptible to security messages and there is less variance in the intentions to adopt them. Second, the channel of influence matters too. The relationship between the susceptibility to privacy influence and the identity of a sender depends on the user's approach to privacy and the ability of the user to carry out the privacy strategy. Indeed, when users have low ability to carry out the privacy behavior, they would rely more on their contacts, while less concerned users will adopt the advice of authoritative organizations. This phenomenon is unique to privacy and points to its divisive properties, which we could not find in messages that promote security.

Altogether, our results suggest that there is a substantial and often overlooked process that helps drive privacy related behavior change, and that in order to maximally raise awareness to privacy, we should think carefully about several strategies, adapting to the privacy approach of potential users. In addition, we believe our work provides a strong foundation for much needed further exploration into the social dimensions of privacy behavior.

ACKNOWLEDGMENTS

We gratefully acknowledge the grant from the Ministry of Science and Technology of Israel and the National Cyber Bureau of Israel, grant number 3-9758, and the contribution of the Blavatnik Interdisciplinary Cyber Research Center, grant number 1-12. We would also like to thank Gal Oestreicher - Singer and Joachim Meyer for their thoughtful comments on this work.

REFERENCES

1. A. Acquisti and J. Grossklags. Losses, gains, and hyperbolic discounting: An experimental approach to

information security attitudes and behavior. In 2nd Annual Workshop on Economics and Information Security-WEIS, volume 3, 2003.

2. I. Ajzen. The theory of planned behavior. Organizational behavior and human decision processes, 50(2):179–211, 1991.

3. S. Aral and D. Walker. Identifying influential and susceptible members of social networks. Science, 337(6092):337–341, 2012.

4. S. Aral and D. Walker. Tie strength, embeddedness, and social influence: A large-scale networked experiment. Management Science, 60(6):1352–1370, 2014.

5. C. J. Armitage and M. Conner. Efficacy of the theory of planned behaviour: A meta-analytic review. British journal of social psychology, 40(4):471–499, 2001.

6. R. H. Baayen, D. J. Davidson, and D. M. Bates. Mixed-effects modeling with crossed random effects for subjects and items. Journal of memory and language, 59(4):390–412, 2008.

7. M. Balestra, O. Shaer, J. Okerlund, M. Ball, and O. Nov. The effect of exposure to social annotation on online informed consent beliefs and behavior. In Proceedings of the 19th ACM Conference on Computer Supported Cooperative Work & Social Computing, CSCW '16, 2016.

8. P. Barberá. Birds of the same feather tweet together: Bayesian ideal point estimation using twitter data. Political Analysis, 23(1):76–91, 2015.

9. V. Barker. Older adolescents' motivations for social network site use: The influence of gender, group identity, and collective self-esteem. CyberPsychology & Behavior, 12(2):209–213, 2009.

10. R. M. Bond, C. J. Fariss, J. J. Jones, A. D. Kramer, C. Marlow, J. E. Settle, and J. H. Fowler. A 61-million-person experiment in social influence and political mobilization. Nature, 489(7415):295–298, 2012.

11. boyd danah and H. Eszter. Facebook privacy settings: Who cares? First Monday, 15(8), 2010.

12. D. Centola. The spread of behavior in an online social network experiment. science, 329(5996):1194–1197, 2010.

13. C. Cheung, Z. W. Lee, and T. K. Chan. Self-disclosure in social networking sites: the role of perceived cost, perceived benefits and social influence. Internet Research, 25(2):279–299, 2015.

14. N. A. Christakis and J. H. Fowler. The spread of obesity in a large social network over 32 years. New England journal of medicine, 357(4):370–379, 2007.

15. N. A. Christakis and J. H. Fowler. Quitting in droves: collective dynamics of smoking behavior in a large social network. The New England journal of medicine, 358(21):2249, 2008.

16. M. J. Darvell, S. P. Walsh, and K. M. White. Facebook tells me so: Applying the theory of planned behavior to understand partner-monitoring behavior on facebook. Cyberpsychology, Behavior, and Social Networking, 14(12):717–722, 2011.

17. S. Das, T. H.-J. Kim, L. A. Dabbish, and J. I. Hong. The effect of social influence on security sensitivity. In SOUPS, pages 143–157, 2014.

18. S. Das, A. D. Kramer, L. A. Dabbish, and J. I. Hong. The role of social influence in security feature adoption. In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing, CSCW '15, pages 1416–1426. ACM, 2015.

19. R. Dey, Z. Jelveh, and K. Ross. Facebook users have become much more private: A large-scale study. In Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on, pages 346–352. IEEE, 2012.

20. T. Dienlin and S. Trepte. Is the privacy paradox a relic of the past? an in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology, 2014.

21. P. Dourish and K. Anderson. Collective information practice: emploring privacy and security as social and cultural phenomena. Human-computer interaction, 21(3):319–342, 2006.

22. J. Fox and J. J. Moreland. The dark side of social networking sites: An exploration of the relational and psychological stressors associated with facebook use and affordances. Computers in Human Behavior, 45:168–176, 2015.

23. J. J. Francis, M. P. Eccles, M. Johnston, A. Walker, J. Grimshaw, R. Foy, E. F. Kaner, L. Smith, and D. Bonetti. Constructing questionnaires based on the theory of planned behaviour. A manual for health services researchers, 2010:2–12, 2004.

24. J. F. George. The theory of planned behavior and internet purchasing. Internet research, 14(3):198–212, 2004.

25. E. Gilbert and K. Karahalios. Predicting tie strength with social media. In Proceedings of the SIGCHI conference on human factors in computing systems, pages 211–220. ACM, 2009.

26. M. Granovetter. The strength of weak ties: A network theory revisited. American Journal of Sociology, 78:1360–1380, 1981.

27. R. Gross and A. Acquisti. Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pages 71–80. ACM, 2005.

28. J. Gunaratne and O. Nov. Influencing retirement saving behavior with expert advice and social comparison as persuasive techniques. In International Conference on Persuasive Technology, pages 205–216. Springer, 2015.

29. U. Hugl. Reviewing person's value of privacy of online social networking. Internet Research, 21(4):384–407, 2011.

30. R. Kang, S. Brown, L. Dabbish, and S. Kiesler. Privacy attitudes of mechanical turk workers and the us public. In Symposium on Usable Privacy and Security (SOUPS), 2014.

31. S. Kokolakis. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 2015.

32. A. Kühberger. The influence of framing on risky decisions: A meta-analysis. Organizational behavior and human decision processes, 75(1):23–55, 1998.

33. L. Lessig. Code and other laws of cyberspace. Basic books, 1999.

34. K. Lewis. The co-evolution of social network ties and online privacy behavior. In Privacy online, pages 91–109. Springer, 2011.

35. K. Lewis, J. Kaufman, and N. Christakis. The taste for privacy: An analysis of college student privacy settings in an online social network. Journal of Computer-Mediated Communication, 14(1):79–100, 2008.

36. M. Madden. Privacy management on social media sites. Pew Internet Report, pages 1–20, 2012.

37. M. Madden and L. Rainie. Americans' attitudes about privacy, security and surveillance. Technical report, Pew Research Center, 2015.

38. 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, pages 340–345. IEEE, 2012.

39. S. Nakagawa and H. Schielzeth. A general and simple method for obtaining r2 from generalized linear mixed-effects models. Methods in Ecology and Evolution, 4(2):133–142, 2013.

40. G. Oestreicher-Singer and A. Sundararajan. Recommendation networks and the long tail of electronic commerce. Available at SSRN 1324064, 2010.

41. S. Patil, X. Page, and A. Kobsa. With a little help from my friends: Can social navigation inform interpersonal privacy preferences? In Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work, CSCW '11, pages 391–394, New York, NY, USA, 2011. ACM.

42. S. L. Pfleeger and D. D. Caputo. Leveraging behavioral science to mitigate cyber security risk. Computers & security, 31(4):597–611, 2012.

43. D. M. Romero, B. Meeder, and J. Kleinberg. Differences in the mechanics of information diffusion across topics: idioms, political hashtags, and complex contagion on twitter. In Proceedings of the 20th international conference on World wide web, pages 695–704. ACM, 2011.

44. P. W. Schultz, J. M. Nolan, R. B. Cialdini, N. J. Goldstein, and V. Griskevicius. The constructive, destructive, and reconstructive power of social norms. Psychological science, 18(5):429–434, 2007.

45. P. Sheeran. Intention—behavior relations: A conceptual and empirical review. European review of social psychology, 12(1):1–36, 2002.

46. F. Stutzman. An evaluation of identity-sharing behavior in social network communities. Journal of the International Digital Media and Arts Association, 3(1):10–18, 2006.

47. F. Stutzman, R. Capra, and J. Thompson. Factors mediating disclosure in social network sites. Computers in Human Behavior, 27(1):590–598, 2011.

48. F. Stutzman, R. Gross, and A. Acquisti. Silent listeners: The evolution of privacy and disclosure on facebook. Journal of privacy and confidentiality, 4(2):2, 2013.

49. N. Wang, J. Grossklags, and H. Xu. An online experiment of privacy authorization dialogues for social applications. In Proceedings of the 2013 conference on Computer supported cooperative work, CSCW '13, pages 261–272. ACM, 2013.

50. 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, pages 763–770. International World Wide Web Conferences Steering Committee, 2013.

51. 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, page 10. ACM, 2011.

52. C. Zhang, J. Sun, X. Zhu, and Y. Fang. Privacy and security for online social networks: challenges and opportunities. IEEE Network, 24(4):13–18, 2010.

APPENDIX

A1. Message Questionnaire

The following questionnaire was attached to each of the posts presented to the participant. Unless indicated otherwise, all items used this scale:

Strongly disagree	Disagree	Undecided	Agree	Strongly agree
1	2	3	4	5

1. I do not trust the person or entity that published the post.
2. I think that the advice is relevant to me.
3. I expect to follow the suggested advice.
4. I do not know how to implement the advice suggested using Facebook's setting.
5. I am willing to press the Like button on the presented post.
6. I do not want to follow the suggested advice.
7. I am willing to share the suggested advice with my friends.
8. I intend to follow the suggested advice.
9. How many of your friends might find this advice relevant? (0, 1-5, 6-10, 11-20, 21-50, 51-100, Over 100)

A2. Exit Questionnaire

The following questionnaire was presented to the participants at the end of the study. The scales were the same as in the message questionnaire.

Demographics

10. What is your gender? (Male, female, other – prefer not to answer)
11. What is your age? (Input field)
12. What is the highest level of education you have completed? (Less than High School, High School, Some college, College Degree, Master's Degree, Doctoral Degree, Professorial Degree)
13. What is your current relationship status? (Single, In a Relationship, Engaged, Married, It's Complicated, In opened Relationship, Widowed, Separated, Divorced)
14. What is your total household income in a year? (Less than $25,000, $25,000-$34,999, $35,000-$49,999, $50,000-$74,999, $75,000-$99,999, $100,000-$124,999, $125,000-$150,000, $150,000 and more
15. What is your country?

Control questions

16. Since which year are you active on Facebook? (Input field)
17. How many hours do you spend on your Facebook account on a typical day? (Input field)
18. How many posts do you publish on a typical week? (Input field)
19. How many friends do you chat on Facebook on a typical week? (Input field)
20. Approximately how many friends do you have on Facebook? (Input field)
21. Why do you use Facebook? Check all that apply for the respective groups: friends, friends of friends, network members, and strangers. (Keeping in touch with people, Finding information about people, Finding information on people's daily lives, Communication, Other)
22. Please indicate all online social networks that you regularly use. (Twitter, MySpace, LinkedIn, Google+, Instagram, Other)
23. Please indicate below your agreement level for each statement.

- a) I know how to change the privacy setting on my Facebook account
- b) Facebook has the privacy controls I want
- c) I care about my online privacy
- d) My friends on Facebook do not care about their online privacy
- e) I saw at least one post or message on Facebook about privacy setting

24. Please indicate below your agreement level for each statement.

- a) I am OK with friends accessing my Facebook timeline.
- b) I am OK with family members accessing my Facebook timeline.
- c) I am OK with colleagues accessing my Facebook timeline.
- e) I am OK with my superiors accessing my Facebook timeline.
- f) I am OK with strangers accessing my Facebook timeline.
- g) It is important to me to protect my identity information.
- h) I am concerned with the consequences of sharing identity information.
- i) I am likely to share my identity information online in the future.
- l) I believe my identity information is well-protected online.

A3. Posts

Posts taken from the page "Social Fixer":

1. limiting who can see your friends list, you can prevent hackers from impersonating you and sending fake friend requests to your friends. This scam is becoming more widespread, and it can trick your friendsinto chatting with someone who they think is you and potentially giving away personal information or being subject to spam. I recommend that everyone change their friend list privacy to something less than the default of "Public".
2. Clicking "Like" may expose you more than you realize... In this great article byLifehacker, they show how Facebook uses your Likes and interactions to promote things to your friends using YOUR name, and how friends may be seeing things youLike that you didn't even realize. So, just think before you Like.

Posts taken from the page "Facebook and Privacy":

3. Earlier this year, Facebook launched a new feature, Graph Search to help you find more of the people, places and things you're looking for and discover new connections based on what others have shared withyou on Facebook. So, if you want to share and still retain your privacy, then you can always review stuff that you've shared on Facebook, change the audience (e.g. public, friend and only me) for your own content and ask others to remove photos or other posts that you tag in.
4. Make Lists for Your Friends. In 2011, Facebook created improved friend lists so that you can customize your settings for different groups of friends. To help you get started, Facebook have already set up three lists for you: Close Friends: Add your best friends to this list to see more of them in your News Feed and get notified each time they post (can be turn off). Acquaintances: People on your acquaintances list will rarely show up in your News Feed. You can also choose to exclude these people when you post something, by choosing Friends except Acquaintances in the audience selector. Restricted: This list is for people youve added as a friend but just dont want to share with, like your boss. When you add someone to your restricted list, they will only be able to see your Public content or posts of yours that you tag them in. Go to your Friends list from your Timeline and you can see which of your friends is on which list. You can also create new customized lists.

5. Remotely log out of your account. You can log out of any Facebook session that you may have left active on another computer or device. If you forget to log out of Facebook and leave the computer, you can log out of the site remotely. But remember that its always safer to log out of Facebook after using Facebook on a public or shared device. From Account choose General Account Settings, then Security Settings. Here, you can view your active sessions and choose to get notified via SMS or e-mail if a new computer or mobile device logs into your account.
6. Limiting Who Can Send You Friend Requests. Have you ever received a friend request from someone you didn't know or didnt want to accept? While Facebook's mission is to give people the power to share and makethe world more open and connected, we also want you to be in control of how you connect with people. To do this, just click the lock icon near the top of your screen, and then click "Who can contact me." If you haven't changed this setting before, you'll see that anyone can send you friend requests, but you can switch it to "friends of friends."
7. Change your Audience after you Share.If you create and share a post or photo with one audience, and later would like to change that audience, you can do so by following these instructions. Use the Audience Selector to change who can see the stuff that you share on your timeline. Remember, if you share content on someone else's timeline or in a group, the owner of that space controls the audience for that post.
8. Control your audience.Whenever you share something on Facebook, you can choose who sees it. You'll find our audience selector tool when you share status updates, photos, videos and other stuff. Just click the tool and select the audience with which you want to share.
9. Privacy Controls for Stories You Share. When you're posting a status update on Facebook, you'll find an audience selector tool near the Post button. This tool lets you choose who can see what you're posting, including on your Timeline, in News Feed, and in search results. Remember, when you post to another person's timeline, that person controls what audience can view the post. Additionally, anyone who gets tagged in a post may see it, along with their friends.
10. Safety Brush Up! Here are a few tips on how to stay safe on Facebook:1. You should never share your Facebook password with anyone.2. Additionally, think before you post.3. Adjust your privacy settings and review them on an ongoing basis.4. Only accept friend requests from people you know personally, and don't be afraid to report things that look suspicious.
11. How do I control what people can find about me? The best way to control what people can find about you is to choose the audience for each of your Facebook posts. 1. Share each post with the people you want to be able to see it. You control this every time you post. 2. Use Activity Log to review individual things youve already shared. Here you can delete things you may not want to appear on Facebook anymore, untag photos and change the privacy of past posts. 3. Ask friends and others to remove anything they may have shared about you that you dont want on the site. You can do this by reaching out to the person directly, or using the reporting feature, also available in Activity Log.