

Influencing Privacy Behavior on Facebook

Master Thesis
Femke Feenstra – Master Student Psychology Consumer & Behavior
Universiteit Twente
s0063711

Supervisor:
Dr. Ir. P.W. de Vries – Assistant Professor Psychology of Conflict, Risk and Safety
Universiteit Twente

2nd Supervisor:
Drs. M. H. Tempelman –
Universiteit Twente

Date: March 28, 2015

Abstract

Given the growing presence of social media such as Facebook and the increased risks to informational privacy associated with social media use, this study investigates if Facebook users can be influenced to change the way they protect their privacy by confronting them with victims of lacking Facebook privacy. Priming participants as members of an In-group associated with the victims is explored as a moderating variable on this effect. Using an online questionnaire of 119 students at Universiteit Twente in the Netherlands, participants were confronted with people experiencing the consequences of their lack of privacy protection on Facebook, in which perceived distance to these people and Self-Categorization of the participants as members of the same In-group as the victims were manipulated. Subsequently the intention to change Facebook privacy behavior was measured but the findings indicate that the proposed effect between the variables could not be confirmed by this study. This might be explained by problems with the setup of the study such as the homogeneity of the sample and the relatively low number of items used to measure constructs. Or perhaps the privacy-paradox, on which the theoretical framework of this study was built, might no longer apply to privacy on rapidly evolving social network sites.

Influencing privacy behavior on Facebook.

Social media platforms and social media websites have grown into an integral part of life for many people. In the past 10 years, social network sites have experienced extreme growth in popularity, reaching every age group and continent, and have provided new opportunities for social behavior and social interaction (Ross, 2014). Social media grew from a social tool to connect and reconnect with people, to an online representation of one's personality available for anyone from friends and family, to complete strangers and (potential) employers.

Facebook has been by far the most used and most active social networking site in the world for years (Statista, 2015). As of December 2014, Facebook had 1.39 billion monthly active users worldwide of which 890 million were daily users (Facebook.com, 2014). In early 2015, in The Netherlands alone Facebook had 9.4 million active users, of which 6.6 million were daily users (Van der Veer, 2015).

Yet over the years Facebook has been repeatedly criticized for lack of privacy protection (Fletcher, 2010). First with the introduction of the "wall" in early 2008, which showed all recent status updates from Facebook connections on a user's start page (Boyd, 2008). Before the wall was introduced other users' statuses could only be found by visiting that user's profile. The introduction of the wall sparked such debate among users that Facebook ultimately decided to offer more options in their privacy settings. But that was far from the last time Facebook was involved in problems surrounding users' privacy. In an 2009 update of their terms of service Facebook claimed all rights to user-uploaded pictures, including the right to use them for commercial means and in-game promotions (Stelter, 2009). Another controversial update was the automatic facial recognition software Facebook added to their site in 2011. This software matched pictures with the people in them and suggested users tag each other in these pictures, which created a visual link between the picture and the tagged user. Once again, this was introduced on an opt-out basis (Milian, 2011). Because of these well-publicized issues with privacy protection, most Facebook users became well aware of the problems Facebook posed when it came to privacy (Boyd & Hargittai, 2010). Yet many users did not use any of the available tools to modify their privacy settings, nor did they use any other means to guard their private information on Facebook (Young & Quan-Haasse, 2013).

Several studies confirmed that employers use social media to search for information about job applicants (Preston, 2011) and a survey among 825 recruiters revealed that 73% of respondents used social media platforms such as Facebook to check up on applicants (Levinson, 2010). However Facebook's users seemed well aware of the possibility of having their future employers view their Facebook profile (Young & Quan-Haasse, 2009). But if Facebook users were aware of their lack of protection of privacy, and of the risks involved in not guarding their privacy, why did they not use the available options to improve their online security? This lead to the main research question of this study: Can Facebook users be influenced to change how they protect their privacy?

Privacy behavior on social media

Facebook's users indicated that they valued their privacy and they were concerned about protecting their personal information while using Facebook. Especially those who had a high need for privacy indicated they were keen to shield their private information from unwanted eyes (Dwyer, Hiltz & Passerini, 2007). But how does privacy work in an online social environment such as Facebook? Privacy is described as the ability of

seclusion of the self or group from others, both concerning the person and their private information (Altman, 1975). Informational privacy can then be explained as a person's or group's right to determine how, when, and in what way personal information is released to another and a pivotal aspect of informational privacy is the desire to keep personal information out of unwanted hands (Westin, 1967). In later research concerning internet privacy it was found that this could also be extrapolated to internet privacy behavior (Buchanan et al. 2007).

Revealing personal information online was found to be the result of carefully weighing cost and benefit (Andrade, Kalcheva & Weitz, 2002) wherein the cost is the offering of private information and the perceived benefit could be anything from social capital or attention to monetary rewards. In stark contrast participants disclosed private information, but they reported disapproval of sharing personal information (Awad & Krishnan, 2006; Debatin, Lovejoy, Horn & Hughes, 2009; Reynolds et al. 2011). This phenomenon of discrepancy between a person's feelings toward privacy and their behavior in information sharing was labeled the privacy paradox (Barnes, 2006), it encompasses the relationship between a person's feelings towards sharing personal information, and their actual behavior in sharing personal information with others (Nordberg, Horne & Horne, 2007).

Protecting Privacy on Facebook

Both frequency and type of Facebook use, as well as internet skill, were found to be related to making modifications to privacy settings (Boyd & Marwick, 2011). However skill was not the only factor in determining online privacy behavior as most users did not change their privacy settings on Facebook even after they had learned how (Govani & Pashley, 2005). Users also willingly posted large amounts of personal information, ranging from basic demographics to politics and sexual preference, and disregarded both the privacy settings and Facebook's privacy policy. 89% admitted that they had never read the privacy policy and 91 % had not read the terms of service (Jones & Soltren, 2005). Males were found to take more risks on average while females were more reluctant to share identifying information online (Fogel & Nehmad 2009). Age was also an important factor in information sharing on Facebook as older individuals reported less information sharing than younger users (Tufekci 2008).

Reducing the reach of their Facebook profile was found to be an often used mean of controlling the Facebook privacy. The diminishment of a profile's audience from "friend of friends" to just friends could also signal a shift in a user's identity orientation since the profile would no longer be available to the public, but merely to those considered friends and acquaintances (Stutzman, 2010). Reducing the audience would be a logical step, as Facebook users reported they mainly use Facebook to keep in touch with their friends (Cheung, Chiu & Lee, 2010) meaning they would have no need for a larger audience of their Facebook profile.

Influencing Privacy Measures

Most research on privacy measures used on Facebook was aimed at privacy measures undertaken at the user's own initiative but several studies have also been conducted to explore the influence of external cues on privacy measures. One study found that when information about risks of privacy disclosures was communicated it made people less inclined to disclose identifying information (LaRose & Rifon, 2007). More recently a study focused on providing a nudge for Facebook users that mentioned how large the audience for their Facebook post was going to be. Participants reported the nudge made them think more about the repercussions before posting to

Facebook (Wang et. al., 2014). Facebook itself used a nudge as a means to point out the new options of privacy protection to their users in 2014. Another mean used to influence Facebook users in their privacy behavior is fear, where users are confronted with the repercussions of not protecting their privacy, a so called fear appeal. A fear appeal is a persuasive message that intends to scare the audience into changing their behavior. It presents a risk, and describes a suggested form of action to prevent harm (Maddux & Rogers, 1983). Though a fear appeal might work on some users, the literature suggested most Facebook users were already well aware of the risks involved.

By some, privacy and privacy management on Facebook were viewed as a collective endeavor. While a person's own privacy attitudes might be reflected in their behavior, other's attitudes towards privacy could be altogether very different and this could influence how they handle other user's personal information. The information users share about one another could have a significant effect on reputation and privacy protection; at times this content may conflict with a person's preferred privacy behavior, or post a threat to one's desired self-presentation (Litt et. al., 2014). The use of Facebook involves trust in those whom private information is shared with to not disclose it further. This "inside threat" of perceived friends sharing their private information had implications for the way users interact with the people in their network on Facebook and on who they would be willing to accept into their network (Johnson, Egelman & Bellovin, 2012).

Self-Categorization

In the 1970's social psychology focused on the behavior of the person as an individual in relation to and within groups (Tajfel, 1970). The social identity theory describes this as a part of an individual's idea of themselves derived by membership of a social group, with the group social identity as a common set of characteristics shared by all members of the group (Turner & Oakes, 1986).

Self-Categorization, as this process of identifying with a certain group is called, states that identity involves several levels of inclusiveness. Humans see themselves as individuals, and as part of several groups of varying magnitudes. These groups were found to have a profound influence on the evaluation of the self (Hornsey, M.J., 2008). The method to determine the minimal conditions under which such a group-membership can form was labeled the minimal group paradigm. Research using this method showed that even arbitrary and meaningless distinctions between groups, such as preferences for certain paintings (Tajfel, 1970) or a favorite football club (Levine et al, 2005), triggered a preference of one's own group over others. With the minimal group paradigm an In-group, the group with which the individual identifies and believes they belong to, could be created with little effort. The In-group was found to be of strong influence on the beliefs and evaluations the individual held of members of the In-group and perceived non-members called the Out-group.

In-group members strive for a positive group social identity and may be threatened by In-group members who don't adhere to the norms or detract from the In-group's positive social identity. To protect the positive group image, In-group members judge other In-group members threatening group identity more harshly than they would members of the Out-group displaying the same behavior, because the members of the Out-group don't threaten their group social identity (Marques, Abrahams, Paez & Hogg, 2001). The extreme judgement of deviant In-group members is called the black sheep effect (Marques, Yzerbyt & Leyens, 1988). High levels of

identification with the members of the In-group and viewing the group as an entity instead of separate individuals were named as factors that fortified the black sheep effect.

Hypotheses and Conceptual Model

As mentioned above, users tended to see the risks of privacy on Facebook as a problem for others, but not for themselves. This seemed odd as, for example, they did report to be aware of potential employers monitoring social media, and of the risks involved with sharing private information online. Perhaps perceived similarities with a “victim” of failing to protect Facebook privacy would establish an effect on the intention to better protect their own Facebook privacy. The following hypothesis was proposed to explore this theory:

Hypothesis 1: Victim Scenario increases the intention to change Facebook privacy behavior when Victim Scenario resembles participant.

But what if this “victim” was someone they perceived to be in their In-group? An In-group seemed to have a great influence on an individuals’ behavior, and on their feelings towards members of their In-group. Perhaps setting an experiment in an In-group setting would influence the results. Thus, the following hypothesis was proposed:

Hypothesis 2: Self-Categorization increases the effect of Victim Scenario on the intention to change Facebook privacy behavior.

The theoretical framework deduced from the literature review and the subsequently proposed hypotheses are visually represented in the conceptual model depicted in Figure 1.

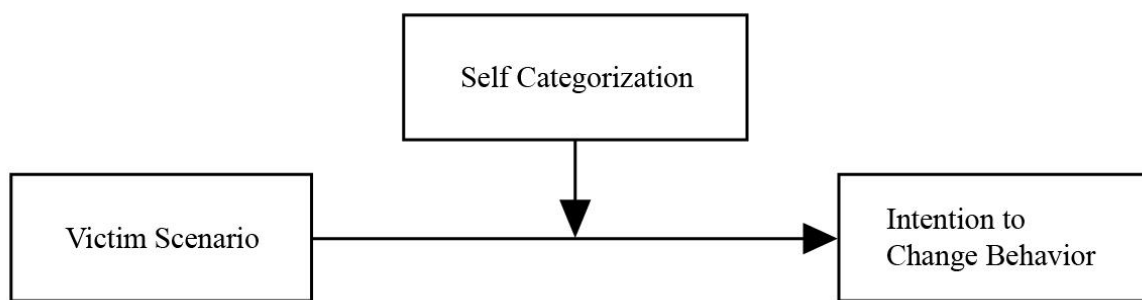


Figure 1: Conceptual Model

Method

Participants and Design

To test this 3 (Victim Scenario: UArticle, UndisclosedArticle, NoArticle) x 2 (Self-Categorization: In-group, Out-group) design an online questionnaire was created and sent to students of Universiteit Twente. In total 121 questionnaires were completed. Participants were selected by inviting them through Facebook, by posting on several Universiteit Twente-oriented Facebook groups, by flyering on campus and by personally approaching students on campus. Participation was voluntary and participants were instructed beforehand. One participant was under 18 years old and was removed from the final sample for reasons of parental consent; another did not have a Facebook account and was removed from the final sample as well. Of the remaining 119 participants, 65 respondents identified as men, while 54 identified as women. Age-wise 66 participants were between 18 and 23 years old, 50 were between 24 and 29 years old and three were aged 30 and up. This survey limited itself to students attending Universiteit Twente to allow for an In-group versus Out-group setup in the experiment. Of the participants 62 were Bachelor students, five were Pre-Master students, 49 were Master students, two were pursuing a PhD and one did not disclose their phase of study.

Procedure

All participants were asked to fill out a questionnaire (Appendix 1). The participants answered questions concerning basic demographics, such as their age and gender, and questions considering their activities on Facebook, for example; “How often do you change your profile?”. The participants also answered a few items on the changing of privacy settings and their awareness of Facebook’s privacy regulations. Participants were also asked how they currently set their privacy settings and if they adapted their type or frequency of posting on Facebook to guard their privacy.

The next segment of the questionnaire concerned the manipulation of Self-Categorization. Half of the participants were asked a few questions about Universiteit Twente students. These were questions such as “Do you think it is important that students at Universiteit Twente protect their privacy on Facebook?” and “Are you currently a student at Universiteit Twente?”. This was done at random to establish half of the participants as members of the In-group of Universiteit Twente students.

Next Victim Scenario was manipulated. Participants were randomly shown either an article about students from Universiteit Twente who got in trouble after sharing too much private information publicly on Facebook (UArticle)(Appendix 2), an article about unspecified people who got in trouble after sharing too much private information publicly on Facebook (UndisclosedArticle) (Appendix 3) or no article at all (NoArticle). As a follow-up to the article, two items were included to establish if the participants identified with the people in the article.

Subsequently all participants were presented with the Inclusion of the In-group in the Self Scale (ISS Scale) (Tropp & Wright, 2001) which showed seven stages of two increasingly overlapping circles and they were asked to select the circles that best described the degree of overlap between them and Universiteit Twente students.

The ISS was shown last to check for the effect of the In-group/Out-group manipulation. The manipulation was also checked by the question “I feel connected to Universiteit Twente” measured on a 7 point Likert-scale.

Finally, the Intention to Change Facebook Privacy Behavior (Intention to Change Behavior) was measured by asking all participants if they were planning on changing the way they handled their Facebook privacy after completing the survey, if so what they were planning on changing, and if not, why not. This measure consisted of one question: “Do you think you will change the way you handle your privacy on Facebook after completing this questionnaire?”.

Two other variables, Skillfulness and Need for Privacy, were measured in the questionnaire; these variables were found to be related to Facebook privacy behavior in the theoretical framework of this study. Skillfulness concerned if the participants felt skillful and at ease while using the internet, both in their knowledge of how to use the internet, and how to manage the privacy risks. The scale used to measure this was derived from previous research on online privacy (Tuunainen, Pitkanen & Hovi, 2009). The scale consisted of five items answered on a 7 point Likert-scale ranging from “Strongly Disagree” to “Strongly Agree” and items included were for example “I feel at ease while using the internet”. This scale reported a reliability of Cronbach’s $\alpha = .74$. A high score for Skillfulness meant the participant felt at ease using the internet and felt protecting your privacy online was important.

Need for Privacy on Facebook (Need for Privacy) was measured to establish how the participants currently acted to protect their privacy on Facebook while using Facebook by answering items on a 7 point Likert-scale ranging from “Strongly Disagree” to “Strongly Agree”. This scale contained eleven items such as “I think before posting something to Facebook” and “I sometimes engage in discussions on Facebook” and was constructed by the author. The scale reported a reliability of Cronbach’s $\alpha = .59$. Two items, “I never post information about my relationship on Facebook” and “I think people judge me based on my Facebook profile”, were removed to increase reliability to Cronbach’s $\alpha = .66$. While this still was not a very high reliability, the inter-item correlation for most items was over .20.

Results

To test the hypotheses a MANOVA was conducted with the Intention to Change Behavior as a dependent variable, Self-Categorization and Victim Scenario as independent variables and Skillfulness and Need for Privacy as covariates.

The main effect of Victim Scenario on the Intention to Change Behavior predicted in the conceptual model was tested but there is no significant evidence to support this effect $F(2, 102) = 1.39, ns$ and therefore Hypothesis 1 cannot be confirmed.

The main effect of Self-Categorization on the Intention to Change Behavior was tested as well but there is no significant evidence to support this effect either $F(1, 102) = 2.35, ns$.

Predicted from the conceptual model is that Self-Categorization has a moderating effect on the influence of Victim Scenario on the Intention to Change Behavior. As $F(2, 102) = 1.19, ns$ there is no evidence of Self-Categorization having a moderating effect and since there is no significant interaction between the two independent variables, this indicates there is no proof for Hypothesis 2.

The manipulation of Self-Categorization was checked by conducting an ANOVA with Self-Categorization as an independent variable and the ISS as a dependent variable. The results show a significant main effect for Self-Categorization. The scores on the ISS are significantly higher for the participants in the In-group, $F(1, 108) = 6.05, p = .02$. This means that those who were primed to think of themselves as Universiteit Twente students report a significantly higher overlap between themselves and Universiteit Twente students. See Table 1 for means and standard deviations.

Table 1. Average scores and standard deviations of connection to Universiteit Twente as a function of the Self-Categorization, and the ISS. Higher scores indicate a higher connection to Universiteit Twente.

Self-Categorization		ISS
In-group	Mean	4.85
	N	52
	Standard Deviation	1.45
Out-group	Mean	4.14
	N	58
	Standard Deviation	1.57

The variables Skillfulness and Need for Privacy were measured for main effects on the Intention to Change Behavior as the literature suggests main effects for both. Skillfulness was added to the MANOVA as a covariate but no significant evidence for a main effect is found $F(1, 102) = 0.48, ns$. Need for Privacy was also tested as a covariate but was not found to have a main effect either $F(1, 102) = 1.11, ns$.

Because of a new privacy update on Facebook all participants had been reminded to check their Facebook privacy by a pop-up message on their Facebook page. This message was shown to all Facebook users in the weeks leading up to distribution of the questionnaire for this study. To measure if the pop-up had any effect the participants were asked if they noticed the pop-up and 62% reported seeing it. Of the participants who reported seeing the pop-up 26% subsequently changed their privacy settings, which means of the entire sample 16% had changed their privacy settings shortly before completing the questionnaire.

A MANOVA was conducted to see if excluding these cases from the sample had any effect on the results but, again, no significant proof for both hypotheses is found with $F(1, 83) = 2.09, ns$ for the main effect of Victim Scenario on the Intention to Change Behavior, $F(1, 83) = 2.22, ns$ for the main effect of Self-Categorization on the Intention to Change Behavior and $F(2, 83) = 0.98, ns$ for the moderating effect of Self-Categorization on the influence of Victim Scenario on the Intention to Change Behavior.

Delving further into the survey results, especially the answers to why the participants reported an unwillingness to change their settings, 80% of participants who were not intent on changing their Facebook privacy behavior

settings stated they had already changed them to protect their privacy. Only 7% said they just did not care about their privacy on Facebook. The other 13% ranged from mentioning they only change it when they have something important coming up to saying it was too much of an effort.

Conclusion

Reviewing the results there was no evidence found for a main effect of Victim Scenario on the Intention to Change Behavior. Therefore Hypothesis 1, “*Victim Scenario increases the intention to change Facebook privacy behavior when Victim Scenario resembles participant.*” cannot be supported by this study. Hypothesis 2: “*Self-Categorization increases the effect of Victim Scenario on the intention to change Facebook privacy behavior*” suggests an interaction effect of Self-Categorization on the influence of Victim Scenario on the Intention to Change Behavior. Again, there was no significant evidence found to support this hypothesis.

The effect of Skillfulness on the Intention to Change Behavior found in the literature review (Marwick & Boyd, 2011) was not replicated in this study. Neither was the effect of Need for Privacy on the Intention to Change Behavior (Govani & Pashley 2005).

Discussion

There is significant evidence for the successful manipulation of Self-Categorization in the experiment and therefore it can be concluded the In-group versus Out-group setup has the desired effect of making the members of the In-group feel a stronger overlap between themselves and Universiteit Twente students than members of the Out-group. Yet there was no significant evidence to support the conceptual model, main research question and proposed hypotheses. Why was there no effect found?

Starting with the theoretical framework, the most surprising result was the inability to replicate the privacy-paradox in this study, as the theory is well-regarded and has been replicated in other studies (Nordberg, Horne & Horne, 2007). One explanation might be that the assumption that the principles of the privacy-paradox, established and replicated in the United States, could be applied anywhere is wrong. The presence and strength of information privacy concerns are partially based in culture (Bellmann, Johnson & Kobrin, 2004) and American research might not be universally applicable. Previous Dutch-German research also failed to replicate the privacy-paradox (Utz & Kramer, 2009). A more realistic explanation of the inability to replicate the privacy-paradox is a theory from 2006, however well-regarded and replicated, might no longer apply in a rapidly evolving field. When the theory was coined there were hardly any social networking sites, Facebook was only available for students and its networks were university-based. Since then social networks have grown and changed tremendously, users have been confronted repeatedly with consequences of lacking privacy protection and have learned to navigate the perils (Lewis, Kaufman & Christakis, 2008). Privacy behavior could simply be catching up to the fast-paced development of online social networks and users’ behaviors could be more in congruence with their attitudes towards privacy (Dienlin & Trepte, 2014). With these possible explanations for the lack of replication of the privacy-paradox and associated research, it might have been unwise to base the

theoretical framework of the study on this theory. Exploring if the privacy-paradox still applies to social network sites makes for interesting future research.

Further exploring the setup of the experiment other limitations come to light. First, the sample used is problematic for several reasons: it was small, as only 119 students participated and with such a small sample it only takes a few participants that strongly deviate from the rest of the sample to skew the results. Another possible issue with the sample is homogeneity. All participants were Universiteit Twente students of roughly the same age, nationality and educational level. As Universiteit Twente is a university that mainly offers technical degrees, and both requires and teaches computer and internet skill, the participants might have been above-average in their Skillfulness and in their proficiency in dealing with internet privacy and security risk. The effect of Skillfulness on the Intention to Change Behavior found in the literature review (Boyd & Marwick, 2011) was not replicated in this study. Most participants in this study report high levels of Skillfulness which made the difference between high-scoring and low-scoring participants on this construct negligible. A more heterogeneous sample with varying levels of education and computer literacy would probably yield different results and would be better suited to take Skillfulness into account.

There are a few issues with the scales used to measure the constructs proposed in the conceptual model. Some of the scales report relatively low reliability levels (below Cronbach's α .7), in part because these scales consist of very few items, and this questions the scales' ability to properly measure the construct. Most importantly Intention to Change Behavior was only measured in one variable; this makes for a very weak measure as there is no way of knowing if it effectively measured the intention to change behavior. Since this was the dependent variable used to test the whole model adding several other variables to measure this construct would have strengthened it considerably.

The reliability of the study on self-reported data poses a problem. The effects of social desirability could have affected the measurement of Need for Privacy and current privacy settings. While the true objective of the questionnaire was not revealed to participants until after the questionnaire was completed they might have inflated their report of the privacy protection measures taken and this could be the reason why the effect of Need for Privacy on the Intention to Change Behavior found in the literature (Dwyer, Hiltz & Passerini, 2007) was not replicated in this study. For future research on Facebook privacy behavior observation by a neutral party is advised as this is the only way to be certain that social desirability has no role in the data.

Another limitation to this study is the use of the article as a means of manipulation. Participants might have merely scanned the article resulting in random answers. Another possibility with more serious consequences for the study is that the participants, especially those in the In-group presented with the UTArticle, perceived the people in the article as a threat to group identity because of their less than favorable actions, therefore negating the desired manipulation effect. This harsh judging of In-group members posing a threat to group identity is the black sheep effect mentioned in the theoretical framework (Marques, Yzerbyt & Leyens, 1988). For future research it might be worthwhile to analyze the influence of Victim Confrontation, or, the effect of seeing others fail, in a more direct and observable way to mitigate such effects.

And finally, right before the questionnaire for this study was launched Facebook displayed a pop-up on all users' homepages to remind them they can change their privacy settings. This means all participants had been reminded to check and update their Facebook Privacy settings in the weeks prior to the study, and 16% of the sample reported changing their settings after seeing the message. In and of itself this might be an answer to the question "Can Facebook users be influenced to change how they protect their privacy", apparently, they can.

References

- Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Monterey, CA: Brooks/Cole Publishing Company.
- Andrade, E.B., Kalcheva, V. & Weitz, B. (2002). Self-Disclosure on the Web: The Impact of Privacy Policy, Reward and Company Reputation. *Advances in Consumer Research*, (29), 350-353.
- Awad, N.F. & Krishnan, M.S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. *Management Information Systems Quarterly* 30 (1), 13-28.
- Barnes, S.B. (2006). A Privacy Paradox: Social Networking in the United States. *First Monday*, 11 (9).
- Bellman, S., Johnson, E. J., & Kobrin, S. J. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. *Information Society*, 20(5), 313–324.
- Boyd, D. (2008). Facebook's Privacy Train Wreck. Exposure, Invasion and Social Convergence. *Convergence: The International Journal of Research into New Media Technologies*. 14 (1), 13-20.
- Boyd, D. & Hargittai, E. (2010). Facebook Privacy Settings: Who Cares? *First Monday*, 15(8).
- Boyd, D. & Marwick, A. (2011). Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies. *Paper presented at Oxford Internet Institute's A decade in internet time, September 22, 2011*
- Buchanan, T., Paine, C., Joinson, A. & Reips, U. (2007). Development of Measures of Online Privacy Concern and Protection for use on the Internet. *Journal of the American Society for Information Science and Technology* 58 (2), 157 – 165.
- Cheung, C. M. K., Chiu, P. & Lee, M. K. O. (2010). Online Social Networks: Why Do Students Use Facebook? *Computers in Human Behavior* 27 (4), 1337-1343.
- Dienlin, T. & Trepte, S. (2014). Is the Privacy Paradox a Relic of the Past? An In-depth Analysis of Privacy Attitudes and Privacy Behaviors. *European Journal of Social Psychology*. doi: 10.1002/ejsp.2049
- Debatin, B., Lovejoy, J.P., Horn, A. & Hughes, B.N. (2009) Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*. 15 (2009), 83–108.
- Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace. *Proceedings of AMCIS 2007, Keystone, CO, USA*. Retrieved July 21, 2014 from <http://csis.pace.edu/~dwyer/research/DwyerAMCIS2007.pdf>.
- Facebook (2014). *Statistics December 2014*. Retrieved March 23, 2015 from <http://newsroom.fb.com/company-info/>
- Fletcher, D. (2010). *How Facebook is Redefining Privacy*. Retrieved June 5, 2014 from <http://www.time.com/time/business/article/0,8599,1990582,00.html>
- Fogel, J. & Nehmad, E. (2009). Internet Social Network Communities: Risk Taking, Trust and Privacy Concerns. *Computers in Human Behavior* 25 (2009), 153-160.
- Govani, T., & Pashley, H. (2005). *Student Awareness of the Privacy Implications when using Facebook*. Retrieved May 1, 2012 from <http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf>
- Hornsey, M.J. (2008). Social Identity Theory and Self-categorization Theory: A Historical Review. *Social and Personality Psychology Compass* 2 (1), 204–222.
- Johnson, M., Egelman, S. & Bellovin, S.M. (2012). Facebook and Privacy: It's Complicated. *Proceedings of the 8th Symposium on Usable Privacy and Security*. Washington, DC, USA.

- Jones, H., & Soltren, J. H. (2005). *Facebook: Threats to privacy*. Retrieved May 1, 2012 from <http://www-swiss.ai.mit.edu/6805/student-papers/fall05-papers/facebook.pdf>
- LaRose, R. & Rifon, N.J. (2007). Promoting *i*-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior. *Journal of Consumer Affairs* 41 (1), 127-149.
- Levinson, M. (2010). *Social Networking ever More Critical to Job Search Success*. Retrieved June 5, 2014 from <http://www.cio.com/article/2417135/careers-staffing/social-networking-ever-more-critical-to-job-search-success.html>
- Levine, M., Prosser, A., Evans, D. & Reicher, S. (2005). Identity and Emergency Intervention: How Social Group Membership and Inclusiveness of Group Boundaries Shapes Helping Behavior. *Personality and Social Psychology Bulletin* 31(4), 443-453.
- Lewis, K., Kaufman, J. & Christakis, N. (2009). The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. *Journal of Computer-Mediated Communication* 14 (2008), 79–100.
- Litt, E., Spottswood, E., Birnholtz, J., Hancock, J., Smith, M.E. & Reynolds, L. (2014). Awkward Encounters of an Other Kind: Collective Self-Presentation and Face Threat on Facebook. *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work and Social Computing*, 449-460.
- Maddux, J. E., & Rogers, R. W. (1983). Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change. *Journal of Experimental Social Psychology* 19(5), 469-479.
- Marques, J. M., Yzerbyt, V. Y. & Leyens, J. (1988). The 'Black Sheep Effect': Extremity of Judgments Towards Ingroup Members as a Function of Group Identification. *European Journal of Social Psychology* 18, 1–16.
- Marques, J. M., Abrams, D., Páez, D., & Hogg, M. A. (2001). Social Categorization, Social Identification, and Rejection of Deviant Group Members. *Blackwell handbook of social psychology (Vol. 3): Group processes* Oxford, UK, Blackwell, 400-424.
- Milian, M. (2011). *Facebook Lets Users opt out of Facial Recognition*. Retrieved May 3, 2014 from <http://edition.cnn.com/2011/TECH/social.media/06/07/facebook.facial.recognition/>
- Nordberg, P.A., Horne, D.R., & Horne, D.A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs* 41(1), 100-126.
- Preston, J. (2011). *Social Media History Becomes a New Job Hurdle*. Retrieved April 12, 2014 from http://www.nytimes.com/2011/07/21/technology/social-media-history-becomes-a-new-job-hurdle.html?pagewanted=all&_r=0
- Reynolds, B., Venkatanathan, J., Goncalves, J. & Kostakos, V. (2011). Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviors. *INTERACT*, 3 (6948), 204-215.
- Ross, M. (2014) *Facebook Turns 10: The World's Largest Social Media Network in Numbers*. Retrieved June 3, 2014 from <http://www.abc.net.au/news/2014-02-04/facebook-turns-10-the-social-network-in-numbers/5237128>
- Statista (2015) *Leading Social Networks Worldwide as of January 2015, Ranked by Number of Active Users in Millions*. Retrieved February 1, 2015 from <http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>
- Stelter, B. (2009). *Facebook's Users Ask Who Owns Information*. Retrieved April 4, 2014 from http://msl1.mit.edu/furdlog/docs/nytimes/2009-02-16_nytimes_facebook_terms_of_service.pdf
- Stutzman, F. & Kramer-Duffield, J. (2010). Friends Only: Examining a Privacy-Enhancing Behavior in Facebook. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2010), 1553–1562.
- Tajfel, H. (1970). Experiments in Intergroup Discrimination. *Scientific American* 223, 96-102.

- Tropp, L.R. & Wright, S.C. (2001). Ingroup Identification as the Inclusion of Ingroup in the Self. *Personality and Social Psychology Bulletin* 27 (5), 585-600.
- Tufekci, Z. (2008). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society* 28(1), 20–36.
- Turner, J.C. & Oakes, P.J. (1986). The Significance of the Social Identity Concept for Social Psychology With Reference to Individualism, Interactionism and Social Influence. *British Journal of Social Psychology* 25 (3), 237-252.
- Tuunainen, V. K., Pitkänen, O. & Hovi, M. (2009). Users' Awareness of Privacy on Online Social Networking Sites – Case Facebook. *22nd Bled eConference eEnablement: Facilitating an Open, Effective and Representative eSociety, Bled, Slovenia*.
- Utz, S. & Kramer, N. (2009). The Privacy Paradox on Social Network Sites Revisited: The Role of Individual Characteristics and Group Norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 3 (2).
- Van der Veer, N. (2015). *Nationale Social Media Onderzoek 2015*. Retrieved March 8, 2015 from <http://www.newcom.nl/social-media-onderzoek2015>
- Wang, Y., Leon, P.G., Acquisti, A., Cranor, L.F., Forget, A. & Sadeh, N. (2014) A Field Trial of Privacy Nudges for Facebook *CHI 2014, Toronto, ON, Canada*.
- Westin A.F. (1967), *Privacy and Freedom*. New York: Atheneum
- Young, A. L. & Quan-Haasse, A. (2009). Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook. *Fourth International Conference on Communities and Technologies, University Park, PA, USA*.
- Young, A. L. & Quan-Haasse, A. (2013). Privacy Protection Strategies on Facebook. *Information, Communication & Society* 16(4), 479-500.

Appendix 1

Geachte Heer/Mevrouw,

Graag nodig ik u uit deel te nemen aan mijn afstudeeronderzoek voor de studie Psychologie aan Universiteit Twente middels deze enquête.

De enquête gaat over Facebook en uw gebruik van Facebook. Het invullen van de enquête duurt ongeveer 10 tot 15 minuten.

Deelname aan de enquête is geheel anoniem en de verkregen data wordt enkel gebruikt voor mijn afstudeeronderzoek. U kunt uw deelname aan de enquête elk moment stoppen door de pagina af te sluiten, pas aan het einde van de enquête worden uw gegevens verzonden.

Alvast bedankt voor uw medewerking,

Femke Feenstra

De volgende vragen gaan over uw demografische gegevens. Selecteer het antwoord dat het meest op u van toepassing is.

Wat is uw geslacht?

- Man
- Vrouw
- Anders

Wat is uw leeftijd?

- Jonger dan 18 jaar
- 18-23 jaar
- 24-29 jaar
- 30 jaar of ouder

Wat is uw nationaliteit?

- Nederlandse
- Duitse
- Belgische
- Anders, namelijk:

In welke studiefase bevindt u zich?

- Bachelorstudent
- Pre-Masterstudent
- Masterstudent
- PhD Student

Heeft u een Facebook Account?

- Ja
- Nee

De volgende vragen gaan over uw kennis op het gebied van internetveiligheid. Selecteer het antwoord dat het meest op u van toepassing is.

Ik voel me op mijn gemak als ik het internet gebruik

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik weet mijn weg te vinden op het internet

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik ben me bewust van de veiligheidsrisico's van internetgebruik

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik maak me zorgen om mijn privacy als ik van het internet gebruik maak

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik vind het belangrijk om mijn privacy te beschermen op het internet

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

De volgende vragen gaan over uw gebruik van Facebook. Selecteer het antwoord dat het meest op u van toepassing is.

Hoe lang heeft u al een account op Facebook?

- Korter dan 1 jaar
- Tussen 1 jaar en 2 jaar
- Tussen 2 jaar en 3 jaar
- Tussen 3 jaar en 4 jaar
- Langer dan 4 jaar

Hoe vaak verandert u iets aan uw profiel op Facebook, bijvoorbeeld uw profielfoto of uw persoonlijke informatie?

- Meerdere keren per week
- Een keer per week
- Meerdere keren per maand
- Een keer per maand
- Minder dan een keer per maand

Selecteer alle soorten connecties die u zelf aan uw Facebook netwerk heeft toegevoegd, meerdere antwoorden zijn mogelijk.

- Goede vrienden
- Vrienden die ik niet tot mijn goede vrienden reken
- Kennissen

- Familie
- Mensen die ik misschien één of twee keer ontmoet heb
- Mensen die ik niet ontmoet heb
- Collega's
- Mijn baas
- Mijn docenten

Selecteer alle soorten connecties die u een vriendschapsverzoek hebben gestuurd, waarbij u het verzoek heeft geaccepteerd. Meerdere antwoorden zijn mogelijk.

- Goede vrienden
- Vrienden die ik niet tot mijn goede vrienden reken
- Kennissen
- Familie
- Mensen die ik misschien één of twee keer ontmoet heb
- Mensen die ik niet ontmoet heb
- Collega's
- Mijn baas
- Mijn docenten

Geef van de volgende gegevens aan of / hoe deze op uw Facebook pagina aanwezig zijn.

Echte naam

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Profielfoto waar u zelf op staat

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Geboortedatum

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Woonplaats

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Adres

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Email adres

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar

- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Telefoonnummer

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Website

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Link naar andere Social Media zoals Twitter, LinkedIn of Instagram

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Genoten opleiding

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Werk

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Huidige status

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Foto's van uzelf

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Foto's van uw vrienden/familie

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Relatiestatus

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Naam van partner

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Sexuele orientatie

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Interesses

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Activiteiten

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Politieke orientatie

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

Religieuze orientatie

- Staat niet op mijn profiel
- Staat op mijn profiel maar is niet up to date
- Staat op mijn profiel maar is bewust onwaar
- Staat op mijn profiel maar is afgeschermd voor iedereen
- Staat op mijn profiel en is up to date en naar waarheid ingevuld

De volgende vragen gaan over hoe u omgaat met Facebook. Selecteer het antwoord dat het meest op u van toepassing is.

Ik denk na voordat ik een bericht plaats op Facebook

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik maak me geen zorgen over de foto's die van mij op Facebook staan

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik denk na over wie mijn berichten kan lezen

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik ga wel eens een discussie met iemand aan op Facebook

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik plaats wel eens een boze reactie op Facebook bij een bericht

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Het interesseert me niet wie mijn profiel bekijkt

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik plaats nooit berichten over mijn relatie op Facebook

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik heb graag een uitdagende profielfoto

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens

- mee eens
- erg mee eens

Het maakt me niet uit wat mensen van mijn profiel vinden

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik vind mijn privacy op Facebook belangrijk

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik denk dat mensen me veroordelen op basis van mijn Facebook profiel

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

De volgende vragen gaan over uw vertrouwen in Facebook en in uw gebruik van Facebook. Selecteer het antwoord dat het meest op u van toepassing is.

Ik maak mij zorgen om mijn privacy als ik gebruik maak van Facebook

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik denk dat de privacy van mijn persoonlijke gegevens beschermd is door Facebook

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik vertrouw erop dat Facebook mijn persoonlijke gegevens niet voor andere doeleinden gebruikt

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik maak me zorgen dat andere gebruikers verkeerde informatie over mij op Facebook plaatsen.

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik vertrouw mijn vrienden op Facebook

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik vertrouw de vrienden van mijn vrienden op Facebook

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik vertrouw de Facebook gebruikers

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

Ik heb vertrouwen in Facebook als bedrijf

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

De volgende vragen gaat over de maatregelen die u heeft getroffen om uw veiligheid te beschermen.

Selecteer de antwoorden aan die op u van toepassing zijn. Meerdere antwoorden zijn mogelijk.

- Ik heb onware informatie over mezelf op Facebook gezet om te voorkomen dat mensen die ik niet ken informatie over mij vinden
- Ik heb informatie over mijzelf weggelaten van mijn profiel om te voorkomen dat mensen die ik niet ken informatie over mij vinden
- Ik kies er voor priveberichten te sturen via Facebook in plaats van het plaatsen van berichten op de Wall van een gebruiker om te voorkomen dat anderen meelesen
- Ik heb voormalige Facebookcontacten geblokkeerd zodat ze mijn profiel niet kunnen zien
- Sommige van mijn Facebookcontacten kunnen maar een klein deel van mijn profiel zien
- Ik wis berichten zodat mensen die niet meer kunnen lezen
- Ik verwijder mezelf uit foto's en berichten waarin anderen mij aanklikken
- Ik maak van geen van bovenstaande maatregelen gebruik

Weet u precies wie welke informatie op uw Facebook profiel kan bekijken?

- Ja
- Nee

Mijn profiel is zichtbaar voor:

- alleen vrienden
- vrienden van vrienden
- iedereen

Bent u zich ervan bewust dat u de privacyinstellingen van uw profiel kunt aanpassen?

- Ja
- Nee

Heeft u ooit de privacyinstellingen van uw profiel aangepast?

- Ja
- Nee

Zo ja, vink hieronder aan welke opties u heeft aangepast, meerdere antwoorden zijn mogelijk:

- Ik heb beperkt wie naar mij kan zoeken op Facebook
- Ik heb beperkt wie mijn profiel kan bekijken
- Ik heb beperkt wie mijn contactgegevens kan zien
- Ik heb beperkt wie mij vriendschapsverzoeken kan sturen
- Ik heb beperkt wie mij berichten kan sturen
- Ik heb ingesteld dat mensen mij niet zomaar in foto's kunnen taggen
- Ik heb ingesteld dat mensen mij niet zomaar in berichten kunnen taggen
- Ik heb ingesteld dat mensen mijn berichten van een tijd geleden niet meer kunnen zien
- Ik heb ingesteld dat mijn informatie niet gebruikt mag worden in Facebook applicaties

Wanneer heeft u de privacyinstellingen aangepast?

- Meteen bij het aanmaken van mijn profiel
- Nadat ik erachter kwam dat ik de privacyinstellingen zelf aan kon passen
- Nadat anderen mij wezen op de openbaarheid van mijn profiel
- Nadat Facebook nadeling in het nieuws kwam op het gebied van privacy
- Na een nare ervaring op Facebook

Heeft u het privacy statement van Facebook gelezen?

- Ja
- Nee

Bent u zich ervan bewust dat Facebook, volgens hun privacy statement, uw gegevens aan derden door mag geven voor marketingdoeleinden?

- Ja
- Nee

Heeft u de gebruikersvoorwaarden van Facebook bekeken?

- Ja
- Nee

Onlangs heeft Facebook de mogelijkheid tot het aanpassen van de privacyinstellingen vereenvoudigd en alle gebruikers daar middels een pop-up bericht over geïnformeerd.

Is het bericht u opgevallen?

- Ja
- Nee

Zo ja, heeft u uw instellingen hierna gewijzigd?

- Ja
- Nee

Vindt u het belangrijk dat studenten hun privacy op Facebook goed beschermen?

- Ja
- Nee

Denkt u dat studenten van Universiteit Twente hun privacy op Facebook goed beschermen?

- Ja
- Nee

Bent u zelf student aan Universiteit Twente?

- Ja
- Nee

U krijgt nu een kort artikel te lezen met betrekking tot Facebook en Social Media. Lees het artikel goed door en beantwoord daarna de laatste vragen.

De volgende vragen gaan over uw reactie op het artikel. Selecteer het antwoord dat het meest op u van toepassing is.

In hoeverre voelt u zich verbonden met de personen in het artikel?

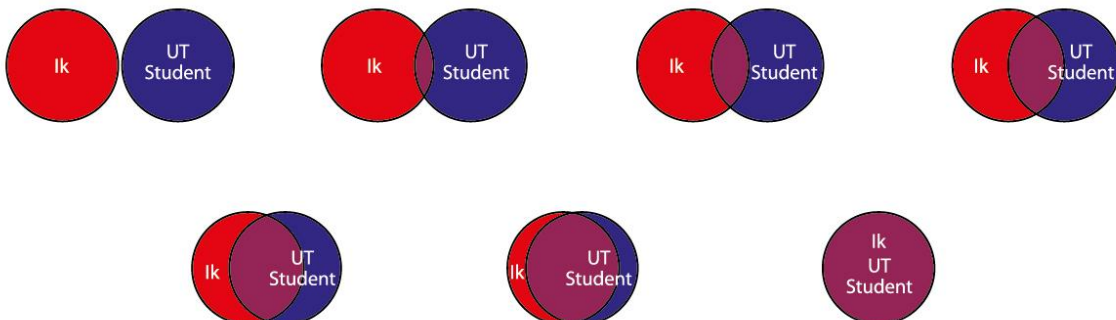
- Helemaal niet
- Niet
- Niet echt
- Weet ik niet
- Een beetje
- Wel
- Helemaal

Heeft u het idee dat wat hen is gebeurd u ook kan overkomen?

- Helemaal niet
- Niet
- Niet echt
- Weet ik niet
- Een beetje
- Wel
- Helemaal

Heeft u na het lezen van dit artikel de neiging uw privacyinstellingen te veranderen?

- Helemaal niet
- Niet
- Niet echt
- Weet ik niet
- Een beetje
- Wel
- Helemaal



Kijk naar bovenstaand diagram. Welke afbeelding geeft het beste weer in hoeverre u zich tot de groep "UT-studenten" rekent?

- Afbeelding 1
- Afbeelding 2
- Afbeelding 3
- Afbeelding 4
- Afbeelding 5
- Afbeelding 6
- Afbeelding 7

Ik voel mij verbonden met Universiteit Twente

- erg mee oneens
- mee oneens
- enigszins mee oneens
- neutraal
- enigszins mee eens
- mee eens
- erg mee eens

De volgende vragen gaan over uw intenties na het invullen van dit onderzoek. Selecteer het antwoord dat het meest op u van toepassing is.

Denkt u dat u na deelname aan dit onderzoek de manier waarop u met uw privacy omgaat op Facebook gaat veranderen?

- Ja
- Nee

Zo ja, wat gaat u aanpassen? Meerdere antwoorden zijn mogelijk:

- Mijn privacyinstellingen
- De hoeveelheid informatie die ik op mijn Facebook heb staan
- Het type informatie wat ik op mijn Facebook heb staan
- Anders, namelijk:

Zo nee, waarom niet? Meerdere antwoorden zijn mogelijk:

- Mijn Facebookinstellingen heb ik al eens veranderd
- Ik vind het niet belangrijk
- Anders, namelijk:

Dit is het einde van de enquête.

Klik hieronder op verzenden om uw enquête in te leveren.

Als u op verzenden klikt is het niet meer mogelijk uw gegevens in te trekken. Alle data wordt anoniem verwerkt dus er is niet meer te achterhalen welke data bij uw enquête hoort.

Hartelijk dank voor uw medewerking.

Appendix 2

Facebook is vaker reden voor ontslag

Sociale media kun je inzetten voor het vinden van een baan, maar ze kunnen je ook je baan kosten.

Werkgevers houden hun medewerkers in de gaten via sociale media en dat leidt tot meer ontslagen, zegt juridisch dienstverlener Arag maandag in het Algemeen Dagblad. Een op de drie bazen zou hun werknemers controleren op Facebook of Twitter. Tien procent controleert zelfs regelmatig.

"Een ondernemer kan gemakkelijk een blik werpen op Facebook of Twitter om te weten wat zijn werknemers in hun vrije tijd uitspoken", zegt een woordvoerder van Arag in de krant. "Veel mensen gooien van alles online en vaak zijn collega's met elkaar verbonden via sociale media. Wie zogenaamd ziek is, maar gisteravond feestend op een foto stond en enkel een kater blijkt te hebben, kan in de problemen komen."

Ook studenten en oud-studenten van Universiteit Twente ondervinden aan den lijve dat bedrijven de sociale media van medewerkers en sollicitanten stelselmatig controleren. Niels (21), een student Bedrijfskunde, werd van zijn stage ontslagen nadat zijn stagebegeleider negatieve opmerkingen over zijn werk bij het bedrijf op zijn Facebook profiel vond. Anne (24), net afgestudeerd in Psychologie zag haar droombaan in rook opgaan omdat er vlak voor het tekenen van haar arbeidscontract ongepaste foto's op haar Facebook pagina bleken te staan, en het bedrijf waar zij wilde gaan werken haar aanstelling daardoor introk.

Volgens Arag nam het aantal arbeidsconflicten in het eerste kwartaal met 20 procent toe, sociale media speelden daarbij een belangrijke rol.

Appendix 3

Facebook is vaker reden voor ontslag

Sociale media kun je inzetten voor het vinden van een baan, maar ze kunnen je ook je baan kosten.

Werkgevers houden hun medewerkers in de gaten via sociale media en dat leidt tot meer ontslagen, zegt juridisch dienstverlener Arag maandag in het Algemeen Dagblad. Een op de drie bazen zou hun werknemers controleren op Facebook of Twitter. Tien procent controleert zelfs regelmatig.

"Een ondernemer kan gemakkelijk een blik werpen op Facebook of Twitter om te weten wat zijn werknemers in hun vrije tijd uitspoken", zegt een woordvoerder van Arag in de krant. "Veel mensen gooien van alles online en vaak zijn collega's met elkaar verbonden via sociale media. Wie zogenaamd ziek is, maar gisteravond feestend op een foto stond en enkel een kater blijkt te hebben, kan in de problemen komen."

Niels werd ontslagen nadat zijn baas negatieve opmerkingen over zijn werk bij het bedrijf op zijn Facebook profiel vond. Anne zag haar droombaan in rook opgaan omdat er vlak voor het tekenen van haar arbeidscontract ongepaste foto's op haar Facebook pagina bleken te staan, en het bedrijf waar zij wilde gaan werken haar aanstelling daardoor introk.

Volgens Arag nam het aantal arbeidsconflicten in het eerste kwartaal met 20 procent toe, sociale media speelden daarbij een belangrijke rol.