Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 164 (2019) 39–47

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies, CENTERIS/ProjMAN/HCist 2019

A Survey on Facebook Users and Information Privacy

Wanda Presthus*, Dina Marie Vatne

Kristiania University College, Department of Technology, Christian Krohgs gate 32, 0186 Oslo, Norway

Abstract

This paper investigates how Facebook users perceive information privacy against the benefits of being a member. Inspired by the privacy calculus model, we created a Norwegian online survey (n=188) in spring 2018 and offer the following insights: The largest benefit of being on Facebook is maintaining contact with friends, and the largest concern is the misuse of identity, not necessarily by Facebook but by third parties. The self-disclosure involved is a privacy trade-off based on awareness, and we argue that our respondents are making an informed decision. The scenario of paying a monthly monetary sum for using Facebook if it means securing their personal data seemed to puzzle our respondents. This study should be interesting for social media users and researchers studying information privacy. While our research mainly confirms existing research, we suggest that this subject could be repeated continuously due to the rapid development and change in both technology and its users.

Keywords: Information privacy; social media; Facebook users; privacy calculus model; online survey.

* Corresponding author. Tel.: +47 22 59 60 00.
E-mail address: wanda.presthus@kristiania.no

10.1016/j.procs.2019.12.152

1. Introduction

Facebook is a social network service that had 2.32 billion members worldwide by the end of 2018 [1]. The sale of advertising space on the site is a significant source of income, and it is an attractive place for businesses to advertise. In addition to the personal data users leave on Facebook, as well as other platforms owned by the network service (including Instagram and WhatsApp), Facebook has access to data from several third parties. Facebook states they do not sell information about their users to others unless the users themselves have approved (www.facebook.com/about/privacy/update). However, several sources find this statement misleading. The Norwegian Consumer Council has pointed out that Facebook gives advertisers access to their target groups based on detailed user profiles. The consequences are the same as if they would have sold the information [2]. In Senate hearings, Facebook CEO Mark Zuckerberg was asked whether he thought consumers have any alternative to Facebook if they no longer want to use the service but still want to fulfill the social need that Facebook satisfies. Many have pointed out that this illustrates Facebook's huge market power, for instance [3] and [4]. The Norwegian Data Protection Authority claims this shows how privacy is important not only on its own but also in maintaining a well-functioning democracy [5]. Due to technological advances, such as Big Data analytics and algorithms, privacy can be lost: *"If technocrats […] have their way, however, we will surrender our privacy without notice and without choice. We can and must resist"* [6 p. 64], and recent research suggests companies adopt codes of conduct, such as *algorithmic transparency* [7].

Nonetheless, having our digital information exploited by commercial operators may have positive consequences [8]. Targeted marketing becomes more relevant and interesting to us as consumers [9]. In addition, having a Facebook account does not cost money. Despite the Cambridge Analytica revelation, free services in exchange for personal data is a trade-off most consumers seem to accept [10]. #DeleteFacebook became a global phenomenon, yet it does not seem the campaign had any impact on most Facebook members [11].

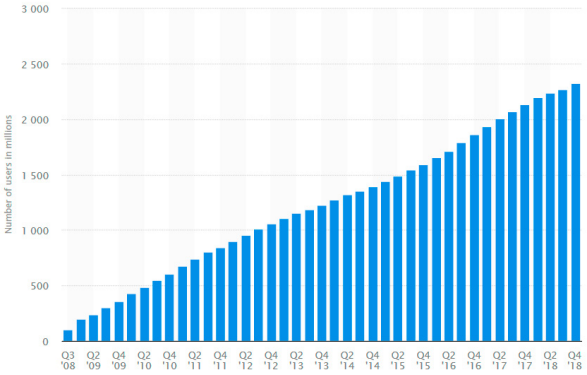


Figure 1: Number of active Facebook users worldwide per month as of the 4th quarter 2018 (in millions). Screenshot from [1].

Figure 1 illustrates the steady increase in Facebook users. Is it because Facebook has become such an important part of our infrastructure and that consumer power is lost because of it? Are the users *locked-in* [12], meaning that the winner takes all because it is too cumbersome to change social media platforms? Or is it rather about the consumers who, despite their high level of awareness about Facebook scandals, do not consider information privacy important enough to set more ultimatums? We narrowed our scope to the following research question: *How do Facebook users perceive information privacy against the benefits of being a member?*

2. Related research

In 1890, Warren and Brandeis defined privacy as the "right to be left alone" [13]. Information privacy is a subset of privacy and concerns an individual's right to control personal data. The simple definition of personal data is any physical or digital data that can be traced back to an individual. This includes a wide range of data from one's name, address, and phone number to more sophisticated things, such as retina scans, voice recognition, and behavior on the web [14]. Today, there are numerous examples of what advanced algorithms can accomplish. For instance, Watson

provides the example of changing one's Facebook status from single to engaged and then automatically getting pop-up advertisements for engagement rings. This is visible to the user, and Watson claims that it will probably score high on the "creepiness scale" (Figure 2).

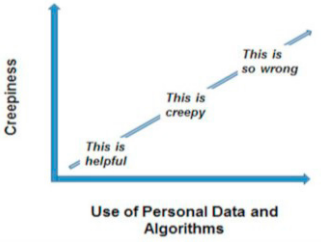


Figure 2: Possible reactions to the use of personal data and algorithms [7 p. 373]

While personalized ads are visible to users, there are many algorithms working behind the scenes. Examples include location discrimination, such as when a user from a wealthy country gets a higher hotel price based on the computer's IP address [9], and the use of web beacons and cookies when browsing online. For example, Presthus and Andersen state that *"Between 100 and 200 cookies are stored on our web browser when visiting the front page of six Norwegian newspapers"* [15 p. 1970]. Pertaining to this fact, Watson and several others have called for *algorithmic transparency*. Facebook is indeed rather open when it comes to technologies and programming code. The open-source technologies include Linux, Apache, MySQL, PHP, Memcached, Haystack, and BigPipe [16]. With or without algorithmic transparency, we find that trust is a recurring issue in the information privacy literature. Trust as a concept has many definitions, but the common denominator is *"an expectation of goodwill"* [10 p. 65]. O'Brien and Torres found that users in general were concerned about their privacy in relation to Facebook and had little trust. However, the lack of trust does not affect the use of Facebook. This phenomenon has been called a *privacy paradox*, but other academics prefer the term *privacy trade-off*. The loss of privacy is accepted because the desire for social interaction is greater [8, 10]. This finding can be tied to the privacy calculus model; self-exposure on Facebook depends on whether or not the benefits will surpass the cost in the form of risking one's privacy [17].

There are numerous conceptual models in the information privacy literature. One of the most common in the information systems (IS) discipline is Mason's PAPA framework [18]. Privacy, accuracy, property, and accessibility (PAPA) are the four ethical issues of the information age, and even though the PAPA framework was created in 1986 it is still highly relevant [15]. We also find that despite its juridical origins, Solove's taxonomy of privacy [19] is highly applicable in the IS context. This taxonomy has four categories: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion. Each category contains examples of harmful activities, such as surveillance, identification, blackmail, and decisional interference. Other risks from a pure networking site perspective, such as cyber-attack risks and privacy abuse risks, have been identified by [20].

According to the literature, the General Data Protection Regulation (GDPR) – a regulation in EU law on data protection and privacy – is playing an increasingly stronger role in information privacy. Implemented in May 2018, the GDPR applies to any company that deals with personal data from users or customers belonging to the European Union (EU) and the European Economic Area (EAA). This means it affects Facebook when it comes to users who are EU and EAA citizens [7, 9].

Summing up the related research, we find that technological advances are facilitating the unprecedented use (and potential misuse) of people's data. There are numerous conceptual models to address this issue. The existing literature has called for research outside the US [13], and we will try to help fill this gap with updated insights.

3. Our method and theoretical framework

We created a survey that returned both quantitative and qualitative data. We drew on the privacy calculus model as a framework for our questionnaire. According to the privacy calculus model,

> *"…a user's decision to become involved in an e-commerce transaction is influenced simultaneously by two sets of contrary factors. The set of inhibitors are Internet privacy concerns and perceived risk. […] The set of drivers are trust, personal interest, and perceived control over personal information submitted. […] The important concept in this model is the cumulative influence of the inhibitors and drivers, forming the so-called 'privacy calculus' (after Culnan & Armstrong, 1999) where each set can outweigh the other,*

determining the user's final decision…" [21 p. 392].

Krasnova and Veltris used a modified version of the model to explore the relationship between trust, benefits, and privacy cost when using a network service [17], as shown in Figure 3.

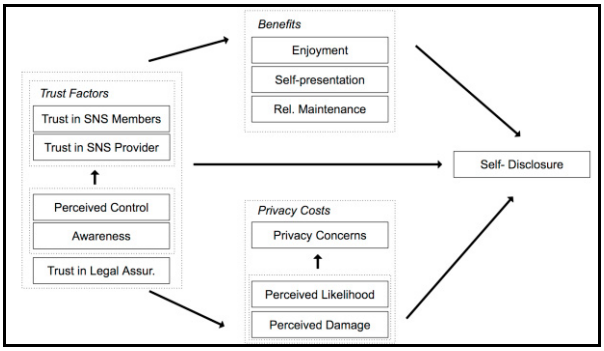


Figure 3. The privacy calculus model [17 p. 3]

We chose to simplify the model in Figure 3. First, we disregarded the arrows because our focus is less about cause and effect and more about revealing insights. Second, we removed some of the variables because they were outside the scope of our study. For example, "Trust in Legal Assurance" was excluded because Facebook's primary business model does not involve payment from the users. Thus, we focused on the following four elements:

3.1 Trust

The privacy calculus model implies that the level of trust depends on perceived control and awareness. Drawing on Krasnova and Veltris [17], we asked our questionnaire respondents to what extent users trust Facebook, whether users have changed the privacy settings, and if users have read the terms of service.

3.2 Benefits

Inspired by Ellison et al. [22], we asked our respondents about the number of friends they have, the main reasons for being on Facebook, and potential positive and negative consequences of deleting their Facebook profile.

3.3 Privacy Cost and Concerns

Inspired by O'Brien & Torres [10], we asked our respondents to what extent users think that Facebook protects their privacy, whether the users have nothing to hide and therefore do not care about their information privacy, and if users would have been more active on Facebook if they had more control over their personal data. There was also an open question about the worst that could happen with the personal data Facebook collects.

3.4 Self-disclosure

In our case, self-disclosure means the actual use of Facebook. We asked the respondents to reflect on what kind of data they are willing to disclose and how much they would hypothetically pay (in money) for being on Facebook if it meant their information would be secure. We also asked the respondents to assess this quote by Zuckerberg: "privacy is over" (Kirpatrick 2010, cited in [6 p. 64]).

The survey took place in April 2018. The link was provided to students at our own university college, but we also provided the link on leaflets that we handed out in the cantinas at the University of Oslo. Lastly, we asked the respondents if they could redistribute our survey to their friends. While we acknowledge the limitations of this convenience sampling and snowballing [23], it nonetheless helped us to reach the population we wanted to study, namely people with a Facebook account. When distributing the survey, we specified that only Facebook members were to participate. Our respondents were anonymous, and we do not know anything about them apart from what they share with us in their answers. The survey questions were in Norwegian, but we observed one answer in Swedish. Altogether, 188 respondents shared their thoughts with us. We analyzed the data by searching for themes and trends [24] and mapped our findings against existing research.

4. Findings and discussion

We discuss our findings using the four categories described in the previous section, but first we present some

background data about our respondents: gender, age, frequency of Facebook visits, and date of joining. (Because none of our questions had a required response and some respondents skipped some questions, our results do not always amount to 100%. Therefore, we do not always include the results in percentage.)

Of the 188 respondents, 104 (55%) are women and 82 (43%) are men. Regarding age, we had four categories based on O'Brien & Torres [10]: under 20 (6 respondents), 20–25 (53 respondents), 26–30 (20 respondents), and over 30 (108 respondents). Our results were somewhat surprising; 108 respondents (57%) stated they were over 30. We expected our majority to be younger and therefore acknowledge that we lose some interesting nuances because 57% of our respondents fall into one age category. We acknowledge that Brian & Torres conducted their study among university population where people usually are younger. However, this finding is congruent with a report that people over thirty are communicating more openly than younger people [25]. The reason for the low number of respondents under 20 is because our survey was distributed mainly to Bachelor and Master students. We asked how often they visited Facebook using four pre-defined categories: daily (156 respondents), weekly (28 respondents), monthly (3 respondents), and less than once a month (1 respondent). We also asked when they became a Facebook member: before 2007 (22 respondents), 2007–2009 (115 respondents), 2010–2013 (23 respondents), 2011–2015 (11 respondents), and after 2015 (4 respondents). In summary, our typical respondent is over 30 years old, visits Facebook daily, and has been a member since 2007–2009.

4.1 Trust

The level of trust was explored using an open question, and 146 respondents provided answers. Of these answers, we could cluster 104 into two groups: OK/much trust (42 respondents) and none/somewhat trust (62 respondents). The comments ranged from being skeptical to having complete trust to or owning responsibility. Some of the comments were: "Ignorance is bliss"; "I acknowledge that everybody will collect data about me"; "Facebook makes their money from selling data. Being on Facebook is entirely voluntary"; "I do not need to have trust"; and "As a Facebook user, it is my own responsibility what I share. Even after the Cambridge Analytica incident".

The responses to our next question "Have you changed the privacy settings because you want more control over your personal data?" were: Yes (98 respondents); No, but I want to (19 respondents); Yes, but for a different reason (24); No (37 respondents); and Do not remember/do not want to answer (9 respondents).

Our last question regarding trust was "Have you read the terms and conditions on Facebook?" The answers were: Yes (18 respondents); All of them or large parts (23 respondents); small parts (71 respondents), and No (72 respondents). In other words, the average participant has some trust, has changed the privacy settings, and has not read the terms and conditions.

Our results agree with O'Brien and Torres [10] in that many respondents do not see the need for trust. One respondent stated that "I do not think about it, so I have quite a lot of trust". Ten respondents explicitly stated that trust is irrelevant. One respondent wrote that "As long as I am a user, this indicates that I have the level of trust that I need". This is an important point; people who have absolutely no trust in Facebook are probably not using it. Our respondents were all Facebook users, and our survey does not reveal any insights from the non-user's point of view. Of the respondents, 72 admitted not reading any of the terms and conditions, and 71 respondents claimed to have read small parts. Not reading the terms and conditions is a common phenomenon, supported by, for example, Obar and Oeldorf-Hirsh [26]; therefore, our findings are not surprising.

4.2 Benefits

We asked how many Facebook friends our respondents have: Under 300 friends (43 respondents [23%]); 300–600 friends (72 respondents [38%]; 600–1000 friends (42 respondents [22%]); over 1000 friends (28 respondents [15%]; and Do not know (3 respondents [2%]). We conducted a cross-analysis to investigate if there was a correlation between number of friends and trust. We would suspect that lack of trust would result in a smaller number of friends, but as Figure 4 shows this is not the case.

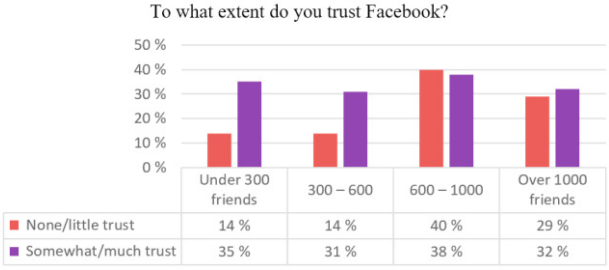
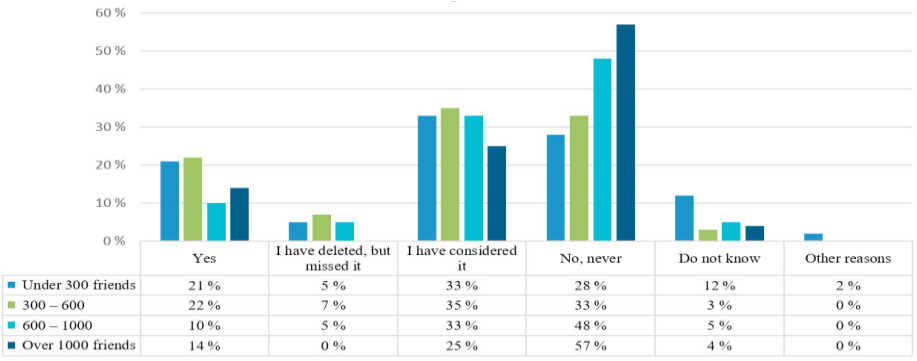


Figure 4. Level of trust versus number of friends: a cross-analysis

The largest group of people who stated that they have none or little trust are the ones who have between 600 and 1000 friends. This finding might be in accordance with the privacy paradox, or it might be that our respondents do not see any conflict between having many Facebook friends and trusting Facebook, meaning that trust is not so relevant in their decision to be a member. We conducted another cross-analysis regarding whether our respondents have thought about deleting their Facebook profile. In this case, we observed a clearer pattern, as shown in Figure 5. We note that the answer "No, never" correlates with the number of friends; that is, the more friends one has, the less likely one is to abandon Facebook. This can indicate the value of maintaining contact with friends and acquaintances.



	Yes	I have deleted, but missed it	I have considered it	No, never	Do not know	Other reasons
Under 300 friends	21 %	5 %	33 %	28 %	12 %	2 %
300 – 600	22 %	7 %	35 %	33 %	3 %	0 %
600 – 1000	10 %	5 %	33 %	48 %	5 %	0 %
Over 1000 friends	14 %	0 %	25 %	57 %	4 %	0 %

Figure 5. Considered deleting Facebook profile versus number of friends: a cross-analysis

We asked an open question about potential positive and negative consequences of deleting Facebook profiles. We clustered the comments into six categories. Of the respondents, 9 (6%) admitted they are addicted to Facebook and that deleting their profile is impossible (the reasons are both work- and school-related); 33 (22%) worry they would have been excluded from social life, such as not being invited to birthdays, if they deleted their profile; 34 (22%) explicitly stated they would completely loose contact with both close and distant friends (friends living far away); and 27 (18%) were concerned about missing important information about school arrangements. Similarly, 29 respondents (29%) thought they would miss getting in contact with new and old friends. Only 20 respondents (13%) claimed that deleting their profile would have no negative consequences. The positive consequences of deleting profiles were less elaborated, but some said that it would "save them time". In summary, most of our respondents had between 300 and 600 friends. The greatest benefit was keeping in touch with friends, and therefore deleting Facebook profiles would be problematic.

4.3 Privacy Cost and Concern

The respondents were asked to assess three statements, as shown below. As Figure 6 illustrates, our respondents mainly disagree with all three statements.

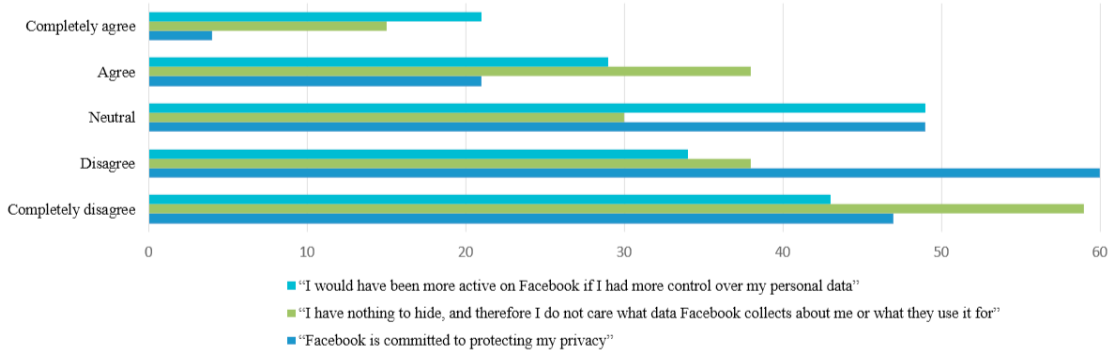


Figure 6: The respondents' assessment of three statements

We asked the open question "What is the worst that can happen with your personal data?" and got 145 responses. Misuse was the top concern and was mentioned by 37 respondents. Some only wrote this one word, while others elaborated by using terms such as identity theft, spam, manipulation, targeted commercials, and surveillance. Some said the data should be sold to a third party. There was a wide range of concerns, and some respondents admitted they were very concerned. For example, one respondent stated that "I dare not think about this". Some worried that their friends might be affected, and others worried that criminals could identify them. Twelve respondents stated that they did not know, and a few said they did not care or were not concerned at all. Our findings are congruent with Solove's [19] and Martin's [9] examples of concern.

In accordance with Bélanger and Crossler [13], we observe that our respondents are indeed concerned about their information privacy, but the benefits surpass the concerns. About one third of our respondents expressed mistrust. Only four respondents completely agreed that Facebook is committed to protecting their privacy, and less than one third stated that they do not care about what kind of data Facebook collects. In addition, over 50% of the respondents have changed their privacy settings. At the same time, only 20 respondents (12%) stated that deleting their user profile on Facebook would not cause problems. This might indicate that many feel they are locked-in [12] to the service.

4.4 Self-disclosure

Our question about what kind of personal data it would be acceptable for Facebook to use for profit had many possible answers, and the respondents could check more than one:

- Information I have given myself, such as gender and age (90 respondents)
- What pages I like, such as companies and public figures (70 respondents)
- Events I am invited to, attend, or are interested in (53 respondents)
- What websites I visit via Facebook (47 respondents)
- What friends I have and when I became friends with them (29 respondents)
- Content from Facebook groups I'm a member of (21 respondents)
- On what posts I "stop" when scrolling down my feed (17 respondents)
- My IP address and thereby my geographical location (15 respondents)
- My whole user history on Facebook (11 respondents)
- Bluetooth signals and thereby my geographical location (7 respondents)
- Information about my friends via my profile (7 respondents)
- Information about saved files on my devices (4 respondents)
- Data collected on me from other websites (3 respondents)
- My phone calls in Facebook Messenger (3 respondents)
- My chat conversations in Facebook Messenger (3 respondents)
- My contact list on my phone (3 respondents)
- None of the above (57 respondents)

Among the 185 responses, as many of 57 respondents stated none of the above. Moreover, our data show that the

users accept that data given on the Facebook site can be used for profit, but that they are more protective when it comes to data that is aggregated from multiple sources.

The following question seemed to puzzle our respondents: "Would you pay for Facebook per month?" The potential answers were: No, I would rather Facebook making money from my personal data (49 respondent); Yes, if less than 2 euros (35 respondent); Yes, if less than 5 euros (25 respondents); Yes, if less than 10 euros (10 respondents); and Yes, over 10 euros (2 respondents). 54 respondents stated that they did not know. In summary, the largest group did not know, followed by those who would not want to pay. For those willing to pay, most would accept the smallest amount, which was less than 2 euros per month.

The open question "Facebook owner Mark Zuckerberg has stated that 'the time for privacy is over'. What are your thoughts on that?" returned a wide range of answers. Some respondents (28) agreed, and some others stated that they felt resigned, saying "He is right. We will never again be completely anonymous" and "RIP privacy". One journalist reporting from the British Parliament went as far as to describe Zuckerberg as a "digital gangster" [27]. We do not want to put any label on Zuckerberg, and nor is the aim of this study to criticize Facebook. As many of our respondents stated, being a Facebook user is voluntary. However, it seems that once one is a member and have accumulated a certain number of friends, it becomes increasingly difficult to leave Facebook.

It can be argued that Facebook has a first mover advantage and that many users feel locked-in [12]. Still, Facebook is not the only social media site, and it will be interesting to follow developments in the near future. There are already some indications that the younger population has other preferences. Finally, Facebook will be affected by the General Data Protection Regulation [7], which three respondents referred to in the open question "Do you have any other comments?" Watson has called for algorithmic transparency, but this was not mentioned by the respondents. Rather, they place the responsibility on themselves in the sense that one should be careful about what one posts on the social media site. Some of our respondents admitted being candid. However, it should be safe to say that it is better to know that you do not know rather than not knowing at all. Our finding is somewhat contradictive to Bandara et al, who found that the decision process in privacy trade-off was influenced by limited knowledge and psychological distance [8].

5. Conclusion, limitations, and suggested future research

This study was guided by the following research question: *How do Facebook users perceive information privacy against the benefits of being a member?* Based on a Norwegian online survey (n=188) conducted in April 2018, we offer some descriptive insights. First, trust played a smaller part than the privacy calculus model indicates. In our study, and our respondents are more concerned with being responsible for what they share. Second, the largest benefit of being a Facebook member is maintaining contact with friends and acquaintances, and the largest concern is the misuse of identity, not necessarily by Facebook but by third parties or criminals. Third, the self-disclosure is a privacy trade-off based on awareness, and we argue that our respondents are making an informed decision. Using Watson's creepiness scale [7] (Figure 2), we place our respondents between "this is helpful" and "this is creepy". None of our respondents seem to think "this is so wrong".

Our study has several limitations, some of which can be addressed in future research. These limitations are: [i] We observe that people over thirty seem to use Facebook in a more carefree way than people below thirty. Therefore, it would be interesting to include more nuances in age (we used 30 years and older) and to analyze how age influences various perceptions and attitudes towards Facebook. [ii] Our findings are not subject to generalization, and nor was this our goal. We offer descriptive insights rather than statistical correlations and cause-and-effect relationships. [iii] Finally, it will be interesting to observe the future of social media in general. Currently, Facebook does not take monetary payment in exchange for their services. Future research could therefore investigate new business models for social media. While our study mainly confirms existing research, we suggest that this subject could be repeated continuously due to the rapid development and evolution in both technology and its users.

The following quote from one respondent sums this paper up well: "I think many are displeased because Facebook has managed to get in a position where the user is locked-in – you have to use their service. We as users have not made an active choice in the way we use, and how much we use, Facebook today. I think this reflects our perception of information privacy. […] Who really cares? Everybody wants to get home to their spouse, or something similar, as fast as possible. The more Facebook can do to ease our lives the less we care."

6. Acknowledgements

We thank our anonymous survey participants for sharing their thoughts on Facebook and privacy, and we are grateful to the three reviewers of CENTERIS 2019 whose thorough comments helped raise the quality of this paper.

References

[1] Statista, *Number of monthly active Facebook users worldwide as of 1st quarter 2018.* Available at: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ [visited April 1st, 2019]. 2019.
[2] Veberg, A., *Tre årsaker til at Forbrukerrådet satte kaffen i vrangstrupen da de leste intervjuet med Facebook-sjefen". [Norwegian]*, in Aftenposten.no, 09.05.2018. (Accessed May 10th, 2018). https://www.aftenposten.no/kultur/i/m6w62g/Tre-arsaker-til-at-Forbrukerradet-satte-kaffen-i-vrangstrupen-da-de-leste-intervjuet-med-Facebook-sjefen. 2018.
[3] Coldewey, D., *'You don't think you have a monopoly?' Read Sen. Graham's delightful grilling of Zuckerberg".* Techcrunch.com, 10.04.2018 (Accessed April 15th, 2018). *https://techcrunch.com/2018/04/10/you-dont-think-you-have-a-monopoly-read-sen-grahams-delightful-grilling-of-zuckerberg/?guccounter=1.* 2018.
[4] Eavis, P., *"Three Takeaways From Mark Zuckerberg's Senate Testimony: DealBookBriefing". Nytimes.com, 10.04.2018 (Accessed April 15th, 2018). https://www.nytimes.com/2018/04/10/business/dealbook/mark-zuckerberg-congress-hearing.html.* 2018.
[5] Nes, C., *"Tre ting vi kan lære av Facebook-skandalen". [Norwegian] Personvernbloggen.no, 20.04.2018 (Accessed May 10th, 2018). Available at https://www.personvernbloggen.no/2018/04/20/tre-ting-vi-kan-laere-av-facebook-skandalen/* 2018.
[6] Few, S., *Big Data, Big Dupe. A little book about a big bunch of nonsense*. 2018: Analytic Press.
[7] Watson, H.J., *Update Tutorial: Big Data Analytics: Concepts, Technology, and Applications.* Communications of the Association for Information Systems, 2019. **44 (21)**: 364–379
[8] Bandara, R., M. Fernando, and S. Akter, *The Privacy Paradox in the Data-Driven Marketplace: The Role of Knowledge Deficiency and Psychological Distance.* Procedia computer science, 2017. **121**: p. 562-567.
[9] Martin, K.E., *Ethical issues in the big data industry.* MIS Quarterly Executive, 2015. **14 (2)**: 67–85.
[10] O'Brien, D. and A.M. Torres, *Social networking and online privacy: Facebook users' perceptions.* Irish Journal Of Management, 2012. **31**(2): 63-97.
[11] Kemp, S., *"Data shows you didn't #DeleteFacebook, so make sure to change these settings". Thenextweb.com, 28.03.2018. (Accessed April 11th, 2018). Available at: https://thenextweb.com/contributors/2018/03/28/data-shows-didnt-deletefacebook-make-sure-change-settings/.* 2018.
[12] Shapiro, C. and H.R. Varian, *Information rules: a strategic guide to the network economy*. 1999: Harvard Business Press.
[13] Bélanger, F. and R.E. Crossler, *Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems.* MIS Quarterly, 2011. **35 (4)**: 1017–1041.
[14] Presthus, W., H. Sørum, and L.R. Andersen, *GDPR compliance in Norwegian Companies.* Norsk konferanse for organisasjoners bruk av IT (NOKOBIT). Svalbard 18-20 September 2018. http://ojs.bibsys.no/index.php/Nokobit/article/view/543/462 Bibsys Open Journal Systems, ISSN 1894-7719, 2018. **26 (1)**.
[15] Presthus, W. and L. Andersen. *Information Privacy from a Retail Management Perspective*. in *In Proceedings of the 25th European Conference on Information Systems (ECIS), Guimarães, Portugal, June 5-10, 2017. pp. 1968-1983*. 2017.
[16] Pingdom. *Exploring the software behind Facebook, the world's largest social media site*. https://royal.pingdom.com/the-software-behind-facebook/ [accessed April 3rd, 2019] 2019.
[17] Krasnova, H. and N. Veltri, *Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA".*, in *Paper presentert at the 43rd Hawaii International Conference on System Sciences, Honolulu, HI, USA*. January 5-8. 2010.
[18] Mason, R.O., *Four ethical issues of the information age.* MIS Quarterly, 1986. **10 (1)**: 5–12.
[19] Solove, D.J., *A taxonomy of privacy.* U. Pa. L. Rev., 2005. **154**: 477–560.
[20] Dinev, T., et al., *Privacy calculus model in e-commerce – a study of Italy and the Unites States.* European Journal of Information Systems, 2006. **4 (15)**: 389–402.
[21] Chena, R. and S.K. Sharma, *Understanding member use of social networking sites from a risk perspective.* Procedia Technology, 2013. **9**: p. 331-339.
[22] Ellison, N.B., et al., *Cultivating Social Resources on Social Network Sites: Facebook Relationship Maintenance Behaviors and Their Role in Social Capital Processes.* Journal of Computer-Mediated Communication, 2014. **4 (19)**: p. 855–870.
[23] Oates, B.J., *Researching Information Systems and Computing*. 2006: Sage Publications Ltd.
[24] Miles, M.B. and A.M. Huberman, *Qualitative Data Analysis*. 1994: Thousand Oaks: Sage Publications.
[25] Marthinsen, S.T. *Brukertallene i sosiale medier. Sosialkommunikasjon.no 17.11.17 [Norwegian] http://sosialkommunikasjon.no/author/sveintore/*. 2018.
[26] Obar, J.A. and A. Oeldorf-Hirsch, *The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services.* Information, Communication & Society, 2018: 1–20.
[27] Stolt-Nielsen, H., *Han anklages for å opptre som "digital gangster" [Norwegian].* Aftenposten, February 20th, 2019.