The Confidence in Social Media Platforms and Private Messaging

Jukka Vuorinen[1], Aki Koivula[2], and Ilkka Koiranen[3]

[1] Unit of Information Systems Science, University of Turku, 20014 Turku, Finland
jukka.vuorinen@utu.fi
[2] Unit of Economic Sociology, University of Turku, 20014 Turku, Finland
akjeko@utu.fi
[3] Unit of Economic Sociology, University of Turku, 20014 Turku, Finland
ilalko@utu.fi

Abstract. In this paper, we focus on social media users and examine the factors predicting users' confidence in platforms in case of private messaging. For the social media platforms, social ties and information that flows through the contacts are valuable assets, which must be considered in the development of the services (such as messaging applications) in order to attract users. We use nationally representative data derived from surveys targeted at 15- to 74-year-old Finns (N = 3,724). The measures included user's confidence in platform services in social messaging, trust in social ties on social media, size of social media networks, a wide selection of measures related to internet and social media behavior, and demographic factors. The results of the analysis supported the hypothesis that high confidence in platforms is strongly dependent on the social resources of users. Network size and trust in social ties were crucial variables in determining the confidence in social media platforms as a secure channel of private messages. The results also amplified that trust in social media networks has independent explanation power in the platform confidence apart from behavioral and demographic factors. The findings are significant in terms of understanding the contemporary information society and dynamics between platform services and users. The markets of social media platforms and other agents in the sector are dependent on the social resources of users, and especially on the social trust of users.

Keywords: Social media, Messaging, Privacy, Trust, Social ties, Survey

1   Introduction

Different messaging applications (e.g., Whatsapp, Facebook messenger) provide a possibility to strengthen and uphold social ties through communication. In the past decade, internet users have seized this opportunity. Mostly, this has put pressure on the reliability and confidentiality of the platforms providing such services including private messages. Privacy makes it possible to deepen and intensify the social relationships especially in terms of sharing sensitive information with a strictly confined and

carefully chosen group of people. More precisely, sharing sensitive information or secrets decreases the social distance between the parties of communication. [1]

From the user point of view, in order to share sensitive information, the service provider needs to be considered as a trustworthy actor, and additionally, the security posture of the platform needs to be seen trustworthy. The reputation of a platform as a reliable actor enabling confidentiality is a significant asset in maintaining the high number of users that is a necessity for the success of the platform. For example, the recent privacy concerns, such as the cases of The Cambridge Analytica and Google+ data leaks, have indicated that the deteriorations of users' confidence in the platform may eventually result in abandoning the services. After the data breach, in which hackers were able to invade Google+'s system, Google announced that they are shutting down the whole platform. In this respect, platforms need to ensure they do not misuse private information themselves and, they need to protect the users' private content from the third parties, such as hackers.

However, despite the recent privacy concerns, the most important social media and messaging platforms are still popular and actively in use, and, to some extent, they have been able to continue to gain popularity in developing countries [2]. This raises the question of whether there are underlying factors that maintain users' confidence in the platform despite the public security risks manifested in protecting of user's privacy. Trust is a tricky phenomenon in terms of how it draws attention. As there is trust, high confidence in the platform, then trust and social ties create and intensify activity on the platforms. Thus, trust brings about content (messages, updates, posts, comments) which in turn creates reactions.

Furthermore, every private message sent through the system (re-)builds and (re-)establishes trust in the system and makes it seem the standard way of communicating. It materializes the fact that the platform is usable in terms of sharing sensitive information. As something becomes repeated it becomes mundane, normal and the standard way of acting. When it becomes the obvious way of acting, it does not draw attention anymore but rather it becomes invisible. Normality, in turn, hinders critical questions about the safety of the service [3]. Thus, as more and more users use a platform, it forms an echoing message of safety. However, when a platform becomes compromised, all the attention is on the platform.

In this study, we seek to catch these vivid social ties by estimating how actively users are engaged to the platform through several attributes. We are interested in how the size of the social media networks and trust in these networks explain the level of confidence in social media platforms. The size of the networks gives us a rough but applicable measure to assess how much potential (social contacts) network contains. In addition, by assessing how much users trust in their social ties gives us another aspect of estimating in how active way users are engaged to these networks. Secondly, we are interested in how different behavioral elements are affecting to interconnections of the level of confidence in social media platforms and primary types of engagement mentioned above. These behavioral elements are measured with the frequency of internet use, the frequency of social media use and skill set for social media use. Additionally, we measure how privacy skills and messaging application preferences are affecting to the level of confidence in social media platforms and primary types of engagement. By

splitting the engagement of users to different elements, we can assess more accurately how different components affect the level of confidence in social media platforms.

2   The Modes of Connection and Interaction

As an individual becomes connected to a social media service, they obtain an unparalleled ability to connect other individual actors. To become a part of social media is to become a part of a collective, an assemblage [4] (see Latour 2005). The ability to connect is the essential dynamics of social media platforms. The platform mediates and makes connections; it is social in the sense of association (Latour 2005). However, social ties (such as a friend connection) that are established on different social media platforms (Facebook) are not always socially active in terms of direct communication, but they may have several different situation and context-dependent functions. In other words, social media is a broad collection of different types of social ties. Moreover, we argue that these ties contain different forms of potential that is possible to be actualized into different kinds of social actions and translated to different outcomes.

However, we are not sure whether it is necessary and accurate to discuss social media "friends" in terms of "social capital", or even resources [5], [6]. At least, for this article, we need to clarify the concepts of a friend, capital and resource. The allegory of "friends as capital" is a slightly problematic analogy because the term capital refers to a stash, a stockpile, savings – something you can quietly go back to, something from which you fetch or draw and then consume. While social media can function as a repository of known friends, it, however, provides merely a possibility to activate a friendship, to re-establish the connection that does not guarantee successful activation by itself. For us, following the line from Georg Simmel [1], to Chicago School of interactionist [7], and Actor-Network theory [4], a friendship is made and enacted through interaction. There is no friendship unless there is an actual exchange, e.g., communication. In other words, a friendship is not a stable property but a constantly becoming process that is acted upon. What is a "friend" that is never contacted? An inert, dead piece in a stockpile? Perhaps it is a perishing acquaintance. Plausibly, it can be both. A hanging friend in a stockpile is in fact a virtual foundation of a friendship that offers a possibility of engaging interactive communication in which friendship becomes actual. Being a friend is an event, not a stubborn structure.

We begin with a premise that in an emerging connection energy flows. The emergence of connection is the initial step of actualization that is the movement of energy. No matter whether it was energy in the form of a message (a rush of electrons) or a thought (a chemical-electric event), a wave of the hand (physical movement), the connection is activated, actualized. A channel is opened. A bridge that connects two banks [8, p. 73]. However, the first act, the initial burst of energy, does not necessarily always lead to reciprocal interaction but the outcome and response is always open, not determinate. This uncertainty materializes in many different ways: a friend might have become different, and thus is not the same as in the past. All the processes are that of nature as they include a piece of unpredictability; p never reaches value 1. "Friend" is

sought to be held together by a stabilizing system that is social media service but there is always nonknowledge and chaos involved, a possibility of transformation [8]. Summarized, between friends energy flows, yet it guarantees nothing but instability.

Regarding social media platforms, the interaction of friends is a necessity for their existence [9, pp. 155–160]. The silence of dried out services such as MySpace, Friendster, Orkut, Google+ forces us to pay attention to what the social in social media is. In simple terms, in alignment with their business logic, the critical factor of being alive is the buzz of users who share, comment, and react. It is noise that users make. The social media platforms and their services also differ in terms of fulfilling users' social needs [10]. Social networking sites, such as Facebook, are merely based on users' self-expression, which is why socialization process often occurs through only following "others" and public commenting [11]. Instead, the messaging applications are more emphasizing on maintenance and development of relationships.

The social is based on activity, on interaction, on the uncertainty of outcome. Previous studies have indicated that the active and intensive use of social media is dependent on the intimacy of user's social interactions [12], [13]. However, users' activity in social media is not straightforwardly related to the intimacy in social relationship manifesting on social media [14]. In other words, activity – for example, messaging – does not always mean sharing sensitive information. Furthermore, the platforms are not only dependent on active social media users, but rather on the integrated and trustful social networks of their users. The platforms breathe through the communication that takes place on them by bridging the social networks of users [15]. Nonetheless, they provide nothing but space and channels for users (to shout out messages and reach other users), which should be - and seems to be - enough to attract more users.

The logic of social media is relatively simple: new users create more noise and call for other users. As the social sites become occupied, they start to hum the noise that is created by the users. The platforms are places of noise that organize, or more precisely that live of the organization of users' noise. Importantly, at this point, using turns around. The user no longer occupies the entitled position of a parasite - the one who merely enjoys services of the host (free space and channels) without paying [8] - but the user becomes a parasitized actor that is drained of information (including reactions) so that they can be analyzed, targeted, fed to algorithms [16]. Through this analysis, the social media service providers cease to be mere internet companies and become advertisement companies selling space for advertisement or selling profiles that is in fact organised noise.

In this sense, social media platforms require and live on the social ties of users to whom the platforms provide a possibility of establishing and maintaining social ties. However, platforms are not static structures on which social action would merely take place, but as mediators, they participate actively as a channel. The place of the channel, the social media platform, lies in between the communicators. It is the place messenger as of Hermes in the Ancient Greek [8]. In an academic discussion, social media platforms have been criticized with concepts of exploitation and alienation.

Initially applied by Marx, "exploitation means the process through which capitalists enrich themselves by selling commodities produced by workers and returning only part of the value of those commodities in wages" [17]. Thus, because users are generally

paid little or nothing in return for the value they create for social media platforms, the rate of exploitation approaches infinity [18]. Alienation on the other hand roughly refers to the process whereby the worker is made to feel foreign to the products of own labor. At this moment, users acting on different social media platforms may not be aware that they are creating value with their social actions on these platforms [19]. In this sense, exploitation and alienation of users can be comprehended as being in mutual dependence on social media platforms.

However, we argue that social media platforms role is not directly comparable with industrial 20th century's capitalist's position, as social media platforms are more dependent from their users. Moreover, it is trust that the sites have to build, and it is not the users that are dependent on their social media hosts. It goes the other way around. Users are hosts. The parasite social site lives attached to the body its victim. The parasite is literally carried around in the pockets of people. The parasite eats processing cycles, reserves memory, drains the battery.

Thus, given the fact that platforms cannot afford to lose their users, some scholars argue that on social media platforms users have to be more likely de-alienated to make the exploitation to happen [17], [19], [20]. Thus, the connection between exploitation and alienation in social media platforms can be understood as some trade-off where users are needed to be de-alienated so that they could implement themselves and gain their full potential in those networking sites [17], [20]. Primarily, by expressing themselves freely, users are producing better - more exciting and alluring - content in both quantitative and qualitative matter, which will eventually turn to more value for platforms. In simple terms, this means more users, more noise to be analyzed, more users to be used.

The social of the media is a link – a string – a social tie. However, in order to keep on the noise of users, social media platform cleverly hides itself. The fuzz is never about the platform itself - it is not the product that is in focus. The focus lies on other users. The channel itself should not get too much attention. As a fluently functioning channel, it becomes almost invisible. The platform came visible and problematized if it does not work or if there are privacy issues. Mark Zuckerberg in U.S. Congress hardly went unnoticed. Moreover, it was because Facebook did not function fluently but was used actively.

Nevertheless, the parasite is invited, and social media is used. Users host it and carry it around. We give it our attention. Admittingly, it provides a neat place for communication, a channel to reach masses. As social media platforms allure users, they provide various services, e.g. private messaging. In terms of actualizing friendship, private messaging is a useful tool. It is no doubt an actualization - a movement of energy - of friendship. Furthermore, what are the energy bursts - the messages - like? In terms of social, they can be sensitive or mundane, the former shrinking the social distance more than the latter. To share sensitive or confidential messages, the user must trust the channel. In other words, in order to make the social gap smaller, the audience of the message must be confined. The secrets that bring people together, bind the ties, are not for everyone but only for a carefully picked number of people. "For your eyes only" is a strong social statement. I want to share this with you. Love excludes. It is only you and me. It

is a decision, it cuts. To include one is to exclude others [8], [21]. Thus, private messaging is required to be trusted regarding that confidential stays confidential.

These notions encapsulate the dynamics of social media platforms; visible social media networks constituted through accepted friend requests or phone numbers added to contact lists are not the bread and butter for platforms, but platforms stay live on social activities that take place on these platforms. Platform cherish by staying under the radar and feast with valuable data streams extracted from these interactions. If nothing is exchanged between users, meaning that social does not materialize, then confirmed ties may stay visible but the platform dies. What would TripAdvisor be without user reviews [22]. The whole social media becomes though activity.

3 METHOD

3.1 Data

Our data based on two different surveys collected at the same time in late 2017 and early 2018. The first part of data were sampled randomly 8000 aged 18 to 74 from the Finnish population register to the mail survey. With 31% response rate, the final data include 2470 observations. Secondly, in order to guarantee sufficient number of social media users, we improved the data by including 1,254 respondents (also aged 18 to 74) from the non-probability sample collected of a nationally representative online panel. Accordingly, the final data included 3,724 respondents, of whom 66% were from the probability sample [23].

In this study, we focused on social media users that accounted for 74 % of the total data. We considered the potential sampling error related to two different data sources by providing a robustness check for the main effects. We also controlled for the demographic bias regarding the age with a weight variable constructed by calibrating the sample's age distribution to correspond with the official population distribution of Finnish social media users according to Official Statistics of Finland [24]

3.2 Measures

Table 1 provides information on the measurements and descriptive statistics for all the variables used in the further analyses. As for the dependent variable, we used a variable elicited from the statement: "I can trust that social media platforms (such as Facebook) will not publicize my messages." The answer options ranged from 1 to 5 in which was given 1 completely disagree, 3 do not agree or disagree, and 5 completely agree. In this study, we recoded the variable as binary by combining categories 1-3 and 4-5 to predict those who agree (initial categories 4 and 5). In other words, we focus on those who can trust the social media platform in private messaging.

Our primary independent variables are the network size on social media and trust in networks on social media. We measured both variables from the same angle using the initial questions "To what extent do you have friends and acquaintances on social me-

dia?" and "To what extent do you trust your friends and acquaintances on social media?". The answer options for both questions ranged from 1 (not at all) to 5 (very much). These variables were used as continuous in further analyses.

We considered for a set of potential confounding variables related to the internet and social media behavior of participants. First, we took into account the general features of internet usage and privacy skills. The frequency of internet usage was measured by asking how often the respondents use internet by using 5-point scale: 1 (never), 2 (less than weekly), 3(weekly), 4 (daily), 5 (many times per day). We asked privacy skills with three different statements after the question "To what extent following Internet actives describe you". Given answers ranged from 1 (Not at all) to 5 (Very well). The initial statements were: 1) I know how to use private browsing settings online (For example, incognito mode) 2) I know how to delete my online browsing history 3) I know how to turn my location services on and off.

Second, to account for the effects of social media usage, we controlled for the participants' social media skills, activity in using social message applications (SMA) and the preferred SMA. Initially, we measured activity by asking the frequency how often the respondents use SMAs with similar scale as in asking the frequency of internet usage. Social media skills were measured by following the validated measure of social skills [25]. We constructed the preferred SMA application by two questions initially asked how often respondents use Facebook and WhatsApp via the same scale from 1 (Never) to 5 (Many times per day). We combined the information of the variables for constructing a new variable to measure whether participants use either Facebook messenger (1), WhatsApp (2), or both of them (3).

We also controlled participants' age, gender, and education throughout analyses. We measured age via an open-ended question in which the respondents reported their year of birth. Education was categorized as binary by differentiating those have achieved at least tertiary level from those having primary or secondary level education.

3.3 Techniques

In the first phase of the empirical study, we assessed the direct effects of that network size and trust in networs on the confidence in social media platform. We also conducted a robustness check for the sample effect by modeling separately for both the probability and nonprobability samples. We conducted the statistical tests by using logistic regression models and presented the results of main effects odds ratios.

We also estimated the indirect effects of independent variables through confounding variables with the KHB tests [26], [27]. The tests were conducted in a step-by-step manner by holding the sociodemographic variables as covariates in each model. We reported the indirect effects in the text as mediation percentages and logit-coefficients. We performed the analyses with Stata 15 by using the KHB -package and illustrated the results by utilizing the user-written packages of coefplots [28] and graphic schemes [29].

Table 1. Descriptive information of the applied measures

Measures	N	M	SD	Min	Max
Dependent:					
Platform confidence in private messaging (binary)	2772	0.26	0.44	0	1
Independent:					
Social resources on social media:					
Social ties on social media	2758	2.87	0.92	1	5
Trust in social ties on social media	2748	3.42	0.95	1	5
Internet and social media behavior:					
*Frequency of usage:**					
Use the Internet?	*2765*	*4.34*	*0.6*	*1*	*5*
Use the Instant messenger applications	*2752*	*3.56*	*0.98*	*1*	*5*
Skills					
Privacy skills (sum variable, alpha = 0.81)	2765	3.76	1.13	1	5
Social media skills (sum variable, alpha=0.88)	2761	4.12	0.85	1	5
Application ***	2760			1	3
Facebook messenger	2760	0.08	0.27	0	1
WhatsApp	2760	0.34	0.47	0	1
Both	2760	0.58	0.49	0	1
Demographics					
Gender	2766	0.52	0.5	0	1
Age	2767	47.9	15.8	18	75
High education	2726	0.59	0.49	0	1

*How often do you do the following?

(1=Never, 2= Less than weekly, 3=Weekly, 4=Daily, 5= Many times per day)

How often do you use the following social media services?

(coded 1=Facebook Messenger, 2= WhatsApp, 3= Both)

4   Results

Table 2 shows the results for the first hypothesis. Social ties had a substantial effect on the confident in social media platform (OR = 1.48 , p < .01). Trust in networks also positively predicted high confidence in the used platform (OR = 1.60, p < .01).

According to the results of robustness check, social ties had similar effects on the probability sample (OR = 1.44, p < .01) and the nonprobability sample (OR = 1.58, p < .01). The effect of trust in networks varies slightly between the probability sample (OR = 1.68, p<.01) and the non-probability sample (OR = 1.47, p<.01). However, according to the interaction analysis, the differences were not statistically significant in either case after the equating of demographic variables.

Next, we added the first set of behavioral variables to the base model. As seen, internet privacy skills and frequency of internet, skills did not affect the association between interest variables and the confidence in social media platform. In addition, the covariate effects of those variables were weak.

Afterward, we complemented the model with the second set of behavioral variables related to social media usage. We found that social media usage skills and frequency of SMAs usage have a positive effect on the confidence in social media platform. Interestingly, internet privacy skills had also negative effect on platform confidence. Finally, those preferred only WhatsApp as SMAs application reported being less likely confident with the platform they used in social messaging.

After conventional logistic regression, we conducted a more in-depth analysis of confounding effects of covariate variables. The results are shown in Table 3. We found that neither the frequency of internet usage nor the privacy skills have confounding effects on the main associations. Instead, the effects of social media usage influenced significantly on both associations. The frequency of SMAs usage confounded 13% of the effect of network size (b=0.05, p<0.01) and 9 % of the effect of trust in networks (b=0.04, p<0.01). Social media skills also confounded the effects of main independent variables; 13 % of the effect of network size (b=0.05, p<0.01) and 11 % of trust in networks (b=0.05, p<0.01). Simultaneously, the preferred application found to be a significant factor, when it confounded over 30 % (b=0.14, p<0.01) of the effect of network size and 15 % of the effect of trust in networks (b=0.08, p<0.01).

Figure 1 illustrates the main results of predictive analyses. We may suggest that the size of social media networks and trust in social media networks positively contribute to the platform confidence of social media users in social messaging. Additionally, we propose that trust in social networks is more effective factor, and not as dependent on the other behavioral factors, as compared to the size of social media networks.

Table 2. Predicting the confidence in social media platform according to the size of social media networks, trust in social ties and covariate variables, Odds ratios and standard errors with statistical significances

Dependent variable:

Confidence in social media platform

	M1	M2	M3	M1	M2	M3
Social ties on social media	1.48**	1.48**	1.25**			
	(0.07)	(0.07)	(0.07)			
Trust in social ties on social media				1.60**	1.59**	1.46**
				(0.08)	(0.08)	(0.08)
Privacy skills		1,01	0.86*		1,02	0.85*
		(0.06)	(0.06)		(0.07)	(0.06)
Frequency of Internet usage		1,09	0,98		1.10	0.98
		(0.1)	(0.09)		(0.10)	(0.09)
Social media skills			1.33**			1.33**
			(0.09)			(0.09)
Frequency of SMAs usage			1.15*			1.16*
			(0.07)			(0.08)
Preferred application: (ref=Facebook messenger)						
WhatsApp			0.49**			0.47**
			(0.1)			(0.09)
Both			1.05			1,08
			(0.2)			(0.2)
Observations	2,707	2,693	2,657	2,698	2,685	2,649

Odds Ratios, Standard errors in parenthese

Models control for age, gender and education

** p<0.01, * p<0.05

Table 3. Effects of social ties and trust in social ties on social media via confounders on the confidence in social media platform, decomposed (KHB) logit coefficients and standard errors.

Dependent variable: Platform confidence in private messaging	Interest variable: Social ties on social media		Interest variable: Trust in social ties on social media	
	B	SE	B	SE
Interest variable's effect via:				
Internet privacy skills	0.002	(0.006)	0.003	(0.005)
Frequency of Internet usage	0.005	(0.005)	0.005	(0.005)
Social media skills	0.05**	(0.013)	0.05**	(0.011)
Frequency of SMAs usage	0.05**	(0.014)	0.0.4**	(0.011)
Preferred application	0.14**	(0.022)	0.08**	(0.013)
Observations	2,707		2,693	

Logit coefficients (B), Standard errors (SE) in parentheses

Models control for age, gender and education

** $p<0.01$, * $p<0.05$
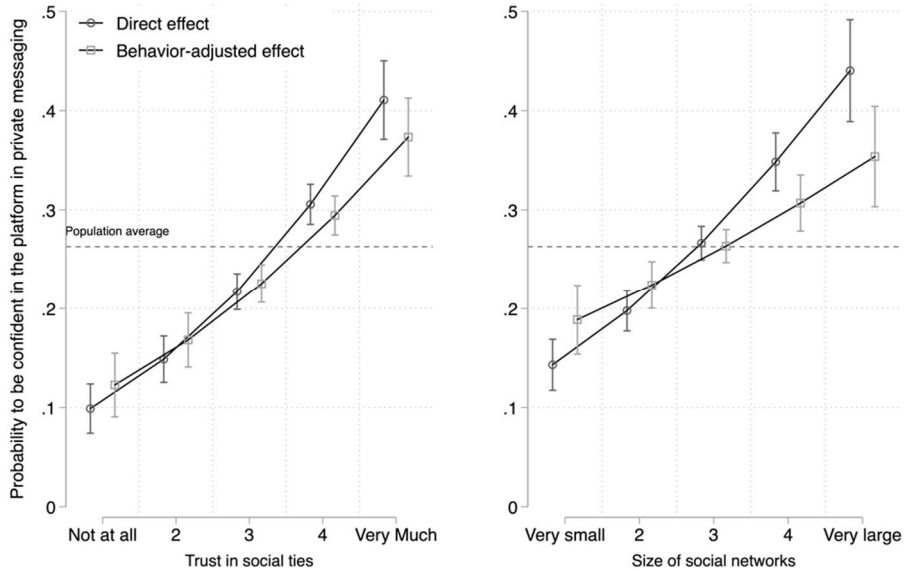
Figure 1. Probability to be confident in the social media platform in case of private messaging according to the size of social media networks (social ties) and the level of trust in social media networks (trust in social ties). Predicted probabilities with confidence intervals.

5   Discussion

First, the results of the analysis support the hypothesis that the high level of confidence in platforms is strongly dependent on how engaged users are to their social networks. The size of network (i.e. the number of social media friends) and trust in the networks were significant variables when we analyzed the confidence in social media platforms as mediators of private messages. Secondly, the results show that trust in social media contacts – friends – has independent explanation power in the platform confidence. Similarly, behavioral elements of engagement, namely frequency of social media platform usage and social media skills, had a positive correlation to the level of confidence in platforms. Additionally, while some may argue that users engaged to these platforms because of high confidence to the platform, the effect is much higher when trust in platforms is used as an independent variable.

The trust in friends seems to go beyond the trust in the platform. In theoretical terms, the importance of actualization itself neutralizes doubts towards the mediating platform. Seizing into the potential of a social tie is always giving up of some privacy. In this sense, technology in between loses its significance if it can deliver the messages seamlessly, in other words, if the platform functions appropriately. We argue, that the trust that is placed in the social media friends and the desire to contact the friends provides such a focus that it blurs the privacy doubts relating to technology. Users' desire to make noise - communicate - suits the mediating social platforms. Every single message brings about data which can be analyzed and thus profited. To be able to use the users, the platforms require data - noise - as much as possible. Thus, the production of data is encouraged. All the platforms are thus inclusive.

However, we should ask who and what is excluded. In a sense, the platforms themselves exclude nothing but people who are unable to use the platform and who are not willing to agree with the terms of use. It is not merely users who can be excluded, but the platforms and some of their features can be excluded from using. As our analysis shows, if the users do not trust in their contacts they exclude the private messaging service or use it more cautiously. The cautiousness with social media friends spreads to the platform as well.

Our analysis also showed that those had a comprehensive set of skills related to privacy issues and are in that sense aware of possible outcomes, do not trust platforms in such extent than those who are not aware of these issues. This notion underlines that when privacy concerns come, visible platform's parasitic role reveals itself. When the platform's role as the active subject is not noticed, users do not feel constraints coming from the third party for their social interaction. Invisibility and insensibility are those features which make both platform and parasite effective; if you do not notice the existence of it, you do not make any actions aiming to dispose of it.

Similarly, trust in platforms associates with platform preferences. Those who favor Facebook Messenger over WhatsApp had significantly higher trust in platforms. Thus, platforms' differences in features related to privacy issues may explain this substantial difference. Since the year 2016 all messages sent via WhatsApp are encrypted end-to-end so that third parties - including WhatsApp itself - are not able to see content [30]. In Facebook Messenger, end-to-end encryption (named as "Secret Conversation") is an optional complement, which user need switch on in every single time when she wants the conversation to be encrypted[31].

As the same company, Facebook Inc. own both of these platforms, it shows how privacy protocols are utilized to lure different segments of users. WhatsApp is bringing privacy issues on the table and is prominently detaching its marketing strategy from the user-generated content (but not from data concerning users networks, ties or frequency of social interaction). Facebook Messenger, on the other hand, is more actively trying to diminish the visibility of privacy issues by for example burying privacy settings in the complex maze of web page architecture. On Facebook Messenger it is possible to encrypt content; to take such action indicates that a privacy issue - the lurking parasite - is recognized. For those are not aware of privacy issues, the presence of a parasite stays hidden.

Our study has some limitations related to the survey period and the interpretation of causality. We conducted the survey before the biggest frenzies in privacy issues faced by Facebook and Google in 2018. By using the applied cross-sectional dataset, we could not validate the mechanism between social media resources and the confidence in the social media platform. This study, however, opened an avenue for further research to focus on how privacy concerns about Facebook and Google have contributed to the association between trust dimensions. We may, for example, ask if it is possible, that trust in social media networks maintain trust in the platform even though the platform has publicly been affected by confidence issues. This hypothesis needs additional development of the applied method by monitoring the variation of participants' trust with longitudinal panel data.

References

1. G. Simmel, *The Sociology of Secrecy and of Secret Societies*. Books on Demand, 1906.
2. Pew Research Center, "Social Media Use Continues to Rise in Developing Countries, but Plateaus Across Developed Ones," 2018.
3. P. Tetri and J. Vuorinen, "Dissecting social engineering," *Behav. Inf. Technol.*, vol. 32, no. 10, pp. 1014–1023, 2013.
4. B. Latour, *Reassembling the Social:An Introduction to Actor-Network-Theory: An Introduction to Actor-Network-Theory*. OUP Oxford, 2005.
5. D. Chambers, "Networked intimacy: Algorithmic friendship and scalable sociality," *Eur. J. Commun.*, vol. 32, no. 1, pp. 26–36, 2017.
6. D. Chambers, "Self-Presentation Online," in *Social Media and Personal Relationships*, 2013, pp. 61–81.
7. H. Garfinkel, *Studies in Ethnomethodology*. Englewood Cliffs, NJ: Prentice-Hall, 1967.
8. M. Serres, "The Parasite," *Clin. Dermatol.*, vol. 10, no. 1, p. 255, 2007.
9. J. van Dijck, *The Culture of Connectivity: A Critical History of Social Media*. Oxford University Press, 2013.
10. A. Quan-Haase and A. L. Young, "Uses and Gratifications of Social Media: A Comparison of Facebook and Instant Messaging," *Bull. Sci. Technol. Soc.*, vol. 30, no. 5, pp. 350–361, Sep. 2010.
11. J. van Dijck, "'You have one identity': performing the self on Facebook and LinkedIn," *Media, Cult. Soc.*, vol. 35, no. 2, pp. 199–215, Mar. 2013.
12. N. B. Ellison, C. Steinfield, and C. Lampe, "Connection strategies: Social capital implications of Facebook-enabled communication practices," *New Media Soc.*, vol. 13, no. 6, pp. 873–892, Jan. 2011.
13. C.-W. (Julia) Hsu, C.-C. Wang, and Y.-T. Tai, "The Closer the Relationship, the More the Interaction on Facebook? Investigating the Case of Taiwan Users," *Cyberpsychology, Behav. Soc. Netw.*, vol. 14, no. 7–8, pp. 473–476, Feb. 2011.
14. A. G. Sutcliffe, J. F. Binder, and R. I. M. Dunbar, "Activity in social media and intimacy in social relationships," *Comput. Human Behav.*, vol. 85, pp. 227–235, 2018.
15. N. B. Ellison, C. Steinfield, and C. Lampe, "The Benefits of Facebook 'Friends:' Social Capital and College Students' Use of Online Social Network Sites," *J. Comput. Commun.*, vol. 12, no. 4, pp. 1143–1168, Jul. 2007.

16. L. D. Introna, "Algorithms, Governance, and Governmentality: On Governing Academic Writing," *Sci. Technol. Hum. Values*, vol. 41, no. 1, pp. 17–49, Jun. 2015.
17. P. J. Rey, "Alienation, Exploitation, and Social Media," *Am. Behav. Sci.*, vol. 56, no. 4, pp. 399–420, Mar. 2012.
18. C. Fuchs, "Labor in Informational Capitalism and on the Internet," *Inf. Soc.*, vol. 26, no. 3, pp. 179–196, Apr. 2010.
19. J. Reveley, "Understanding Social Media Use as Alienation: A Review and Critique," *E-Learning Digit. Media*, vol. 10, no. 1, pp. 83–94, Feb. 2013.
20. E. Fisher, "How less alienation creates more exploitation? audience labour on social network sites," *TripleC*, vol. 10, no. 2, pp. 171–183, 2012.
21. O. Pyyhtinen, *The Gift and its Paradoxes*. 2014.
22. W. J. Orlikowski and S. V Scott, "What Happens When Evaluation Goes Online? Exploring Apparatuses of Valuation in the Travel Sector," *Organ. Sci.*, vol. 25, no. 3, pp. 868–891, Dec. 2013.
23. J. Sivonen, A. Koivula, A. Saarinen, and T. Keipi, *Research report on the Finland in the Digital Age -survey*. Turku: University of Turku, Department of Social Research, 2018.
24. Official Statistics of Finland, "Use of information and communications technology by individuals," 2016.
25. A. J. A. M. van Deursen, E. J. Helsper, and R. Eynon, "Development and validation of the Internet Skills Scale (ISS)," *Information, Commun. Soc.*, vol. 19, no. 6, pp. 804–823, Jun. 2016.
26. R. Breen, K. B. Karlson, and A. Holm, "Total, Direct, and Indirect Effects in Logit and Probit Models," *Sociol. Methods Res.*, vol. 42, no. 2, pp. 164–191, May 2013.
27. K. B. Karlson, A. Holm, and R. Breen, "Comparing Regression Coefficients Between Same-sample Nested Models Using Logit and Probit: A New Method," *Sociol. Methodol.*, vol. 42, no. 1, pp. 286–313, 2012.
28. B. Jann, "Plotting regression coefficients and other estimates," *Stata J.*, vol. 14, no. 4, pp. 708–737, 2014.
29. D. Bischof, "New graphic schemes for Stata: plotplain and plottig," *Stata J.*, vol. 17, no. 3, pp. 748–759, 2017.
30. WhatsApp Inc., "WhatsApp Security. Privacy & Terms protocol," 2018. [Online]. Available: https://www.whatsapp.com/security/ .
31. Facebook Inc., "Help Center," 2018. [Online]. Available: https://www.facebook.com/help/.