IADIS International Journal on WWW/Internet
Vol. 16, No. 1, pp. 56-69
ISSN: 1645-7641

TRUST AND PRIVACY IN MESSAGING

Jukka Vuorinen, Aki Koivula and Ilkka Koiranen
Economic Sociology, Department of Social Research, University of Turku, Finland

ABSTRACT

Internet related personal communication has increased significantly in the course of recent years. Simultaneously, the possibility of sharing sensitive personal information has become a part of everyday life. Thus, the possibility of privacy violations and leaking of personal data has arisen. This paper analyzes the extent to which Internet users trust that the privacy of their private messages is protected and upheld in web-based messaging services such as Facebook Messenger and WhatsApp. The paper examines how users' trust in other people (social trust) and trust in institutional actors (such as the parliamentary system and police) predict a high probability to trust that their private and confidential messages are not disclosed. The analysis is conducted based on data (n=1648) that was gathered through a nationwide survey in Finland. Results show that both high social trust and institutional trust are associated with high trust in the confidentiality and privacy of messages that are sent through messaging services on the web. Demographic factors did not have a remarkable effect on how trusting users are. Finally, a decomposition analysis shows that social trust is the strongest predictor even when institutional trust and demographic factors are controlled for.

KEYWORDS

Privacy, Trust, Social media, Messaging, Communication

1. INTRODUCTION

New communication technologies and services have vastly changed the ways in which people interact socially. Various social Internet platforms have improved and extended opportunities for communication and interaction. For some, social media is a platform for affecting the opinions of thousands or seeking validation through modifying visual self-presentation and taste expression, while for others it is used for routine relationship maintenance and interaction (e.g. Keipi et al., 2018). This has also generated a great deal of pressure towards ensuring the reliability, confidentiality, and integrity of these platforms.

Simultaneously, while a growing share of the population has embraced these novel means of social interaction, the societal significance of social media platforms has skyrocketed. Nowadays, companies providing these new spaces of interaction mediate most of the messages that are sent through the Internet. For example, Facebook Messenger and WhatsApp combined mediate 60 billion messages per day (Tynan, 2016). This also means a great burden of responsibility for these social media giants in terms of securing the privacy of messages.

The value and profitable growth of social media platforms are highly dependent on the number of users. Therefore, the reputation of a platform as a trusted and safe actor becomes one of its most significant assets. For example in recent cases, such as Cambridge Analytica's misuse of the data collected from Facebook in March 2018 (Confessore, 2018; Kang and Frenkel, 2018) and large-scale data breach from extramarital affair dating site Ashley Madison in July 2015 (Dewey, 2016; Victor, 2015), the reputation of the platforms became damaged and many users expressed their distrust by abandoning the service. In this sense, platforms need to firstly ensure that they do not misuse private information themselves and secondly, they need to ensure that third parties, such as hackers, do not gain direct access to private content. In this respect, from the user point of view, the service *provider* needs to be considered as a trustworthy actor and additionally *the security posture of the platform* needs to be seen as trustworthy.

In addition to the service provider, there is also another actor that can violate privacy, namely the *receiver(s)* of a message. Other participants are able to redistribute sensitive content to third parties or in some cases the content receiver is even able to blackmail the sender by threatening to publish this content. In the course of this century, there have been several examples where a known or unknown receiver has leaked sensitive content to third parties or to the media. For example, many politicians and other celebrities have been caught "sexting", namely sending messages written with sexual language or sending sensitive pictures via a mobile phone or other electronic devices to certain receiver(s) (see Juntunen and Väliverronen, 2010). While many of these cases have essentially been sexual harassment, these recent examples illustrate the fact that receiver(s) might publish content of the message to others.

The risk of someone leaking private or sensitive content doesn't solely concern politicians or celebrities. For example, so called "revenge porn", where someone intentionally tries to embarrass others through posting online identifiable and sensitive content which was originally meant only for the receiver, has been growing during the social media era (see Stroud, 2014). In this respect, the interplay between risks, trust and social action contains several different actors – namely the platform, the platform's security and the receiver all of whom need to be trusted before private interaction can be established in a secure way.

Thus, there is a need for a population-level study of citizens' perceptions regarding trust in private interaction on social media. Fundamentally, we are interested in users that communicate privately over the web using different messaging and communication services. Here, we do not solely refer to social media platforms, but comprehensively also to more conventional means of interaction such as emails, discussion forums and chat messaging. Moreover, we are curious about users' trust in the strength of message privacy and confidentiality, i.e. how confident users are that this kind of messaging will remain private. As such, we ask the following research question:

1. *How confident (i.e. trusting) are users that their confidential and private messages are kept private?*

Furthermore, we explore how high trust in message privacy is associated with the two forms of trust, namely institutional trust and social trust. Briefly, institutional trust refers to how citizens trust their governmental actors such as the parliamentary system and police, whereas social trust designates general trust placed in other individuals. Social trust refers to how an individual trusts in other individuals that are solely categorically known. For example, how a customer in a grocery store trusts other customers and their intentions.

On the one hand, these two forms of trust, social and institutional, have drawn significant attention in the field of social sciences. It is suggested that at the micro-level social trust promotes, for example, positive effects on happiness (Inglehart, 1999), health (Subramanian et al., 2002) and ethnic tolerance (Dinesen and Sønderskov, 2013). At the macro-level, nations reporting high levels of trust also tend to perform better in terms of social equality, levels of corruption and economic growth (Bjørnskov, 2012; Rothstein and Uslaner, 2005). Many studies have suggested that low corruption and trust in the fairness of institutions are still essential in the accumulation of social trust (e.g. Dinesen and Sønderskov, 2013; Nannestad et al., 2014; Rothstein and Stolle, 2008). Overall, it can be argued that these forms of trust are crucial determinants in all relations making daily life easier and helping to meet desired expectations (e.g. Coleman, 1988; Möllering, 2006; Rothstein, 2005; Freitag and Traunmüller, 2009).

On the other hand, privacy issues have been a common concern in the field of information system sciences (e.g. Gross and Acquisti, 2005; Ellison, 2007). However, in these cases, privacy is mainly a concern at the platform level (how much a system gathers private information and how this information is exploited). Thus, it is important to examine trust in message privacy and compare it to institutional trust and generalized social trust in order to better gauge these contributors to users' wellbeing. In other words, we hope to show how social and institutional trust is associated with the perceived confidentiality of private messaging in digital media. We explore whether social and institutional trust are apparent in predicting citizens' concern about Internet security by asking:

2. *To what extent does high social and institutional trust predict individuals' high trust in the protection of the secrecy of their private messages (i.e. respondents trust that their messages will not go public)*

In recent research, the use of web services such as digital media has been shown to be linked to various contextual factors. For example, it has been shown that younger, highly educated and those living in urban areas are more likely to use social media compared to others (e.g., Keipi et al., 2018; Schradie, 2011; van Dijk, 2005). Similarly, young and highly educated people are also more skilled in Internet use and online media for different use purposes, for example in effective communication (Hargittai, 2010; van Deursen and van Dijk, 2011). In this respect, these active users might have a better understanding and more experience on which trust (or distrust) can be formed (van Dijk 2005, 71-93). In addition, highly educated and well-off people tend to report both higher social trust and higher institutional trust than others (e.g., Helliwel and Putnam, 2007; Kouvo, 2014, 24; Listhaug and Ringdal, 2008; Rohrschneider and Schmitt-Beck, 2002). Together, these results concerning the association between demographic background, different forms of trust and the use of digital technology and communication services spur us to assume that the associations between trust dimensions (social and institutional) and trust in the confidentiality of private messages are partly dependent on the demographic factors of users. Accordingly, we also ask:

3. *To what extent is the interplay of trust dimensions determined by demographic factors?*

Before moving into empirical testing, we present the framework of the study by explaining essential concepts and formulating a theoretical link between the different forms of trust. We then describe the data and methods of analysis. Finally, after the results section, we discuss the implications of our findings by considering potential limitations and further research avenues.

2. TRUST, EXPECTATIONS AND CONFIDENTIALITY OF PRIVATE MESSAGES

Messages that are sent through social message platforms can be assessed in terms of security through the three dominating concepts in the field of information security, namely confidentiality, integrity, and availability. More specifically, confidentiality pertains to actors who are allowed to access a specific piece of information (or a web based service). Integrity pertains to the order of the message and how it remains the same throughout the process of sending and receiving. (Vuorinen and Tetri, 2012.) For example, the order of letters should not mix in the process but stay exactly the same. Availability, in simple terms, means that the service (and thus the message) should be accessible when needed. In terms of our study, the dimension of confidentiality is the most significant as we are interested in how confident respondents are that their messages will remain private. In other words, how confident users are that the message will be seen solely by the receiver(s) and the message will not be made public.

Trust can be a challenging property to measure directly in the context of socio-techno-material assemblages because "trust" is a strong social notion that is often related to a belief that someone (instead of something) will do something. As Ermisch et al. (2009) put it, "We trust when we trust that someone will do X— repay a loan; arrive on time; play fair; pay the fare; feed the cat; treat baby well; do his job as expected. The trust that we have in someone doing X does not necessarily extend to trust in that same person doing Y." Here, trust is a human bonding word. Although we do not consider that agency would be a solely human property (Latour, 2005) we find it more relevant to approach trust through expectations (Mayer et al., 1995; Blomqvist, 1997; Rousseau et al., 1998; McEvily et al. 2003).

Sociologist Erving Goffman (1986) argues that every time an individual enters a new situation, they have to answer the question of "what is going on here?". So, the answer can be "it rains", "a child is playing", "a computer crashes". Thus, Goffman's frame is a description, an explanation or an account of the current situation (see also Garfinkel, 1967). However, the frame does not merely cover the present but there is also a teleological dimension to it. This teleological frame is an expectation of what will happen, what will follow. For example, if one becomes surprised, it means that something unexpected took place and the teleological frame was broken. However, expectation comes with uncertainty – it is a prediction. For example, a user of an IT device can expect an application to run smoothly but might not be extremely surprised if it crashes. However, if the device itself crashes in such a way that it cannot be rebooted, the feeling of surprise is certainly more intense. To put it slightly differently, expectation is a teleological frame of trust; it designates how X is believed to happen. Expectation is trust in terms of certainty (see Latour, 2005; Luhmann 1995).

In relation to messaging systems, expectation can be used as a subtle way to measure trust. "I expect my messages to stay private (confidential)" is a teleological frame that refers to what is believed to happen and implies trust/non-trust. There is a possibility that the message will be leaked by the relaying system or by the receiver, but here trust makes the difference in whether the message is sent. Trust can vary significantly (Blomqvist, 1997; Sztompka, 1999). In everyday life, social trust is a common and central feature. We usually have high social trust in people that are close to us, with whom we live for example. So, I trust that my colleague will finish a task that they have promised, or within a family unit everyone can trust each other in a certain fashion. However, there is a more peculiar form of social trust, namely generalized social trust. Generalized social trust refers to trust in people that we do not know directly (Kouvo, 2014). They are individuals that we do not know but travel, consume, and live with us.

In social action trust is not only based on social trust between the actors, but also on wider forms of trust (Lewis and Weigert, 1985, 973). Institutional rules, social norms, contracts and laws are defining what is legitimate and thus what outcome is expected (Rousseau et al., 1998, 400). In this sense, societal structures can be seen as important sources of *institutional trust* that are streamlining all social processes and actions occurring in societal contexts. Accordingly, institutional trust can be comprehended as feature adopted through socialization and additionally quality of the societal context itself (Kouvo, 2014, 22). According to this, it isn't surprising that generalized social trust and institutional forms of trust are highly linked to together (see Rothstein and Stolle, 2002, 7). In this respect, effective realization and supervision of institutional rules, norms, contracts and laws by governmental institutions can be seen as important source for social media users' exceptions and trust that platform providers and also other users are acting properly, ethically and in accordance with the law.

The most recent concerns have been raised about institutional privacy especially in terms of the use of personal data by institutions. This is relevant for policy discussions, as it firstly suggests that the collection, aggregation, and utilization of personal data for targeted advertisement has become an accepted social norm (Young and Quan-Haase, 2013). Secondly, different platform companies', such as Google and Facebook, potential societal power has substantially accelerated during this decade. Nowadays big platform companies possess and process private information and messages from billions of people. In this respect, these platform providers have a special status in the discussion about privacy issues in the social Internet.

Recent data breaches, such the case of Facebook and Cambridge Analytica and also the case of Ashley Madison, have had major consequences to users' feeling of trust. These breaches appeared as disruptions which made risks visible, and through lowering feeling of trust they eventually also harmed platforms themselves due the lowering brand reputation and revenues. Through this dependence between users' trust and platforms economic performance, platform companies have been trying to restrain harmful actions of other users. For example, in November 2017, Facebook asked users who are afraid that some might distribute their private photos to send these photos to the company so that re-upload can be blocked on company's different platforms, namely Facebook, Messenger and Instagram (Solon, 2017). In this sense, actions of the platform company are claimed to improve their technology, services and security. In terms of trust, there is an interesting and important feature in it: if a user sends a sensitive photo to Facebook in order to prevent its later use as a tool of humiliation on Facebook owned platforms, then sending a photo can be seen as materialized trust. In other words, the user trusts sensitive material on the hands of company in order to prevent misuse

by other users. In simple terms, this means that the platform itself is trusted. In fact, providing such services or features, platforms seek to improve their credibility and restore or strengthen users' trust.

When different aspects behind users' trust in the protection of the secrecy of their private messages are divided and recognized on a conceptual level, social communication and interaction online show themselves as more complex and multilayered than they appear to be initially. As such, it is important to empirically study how different aspects of trust are affecting users' trust that their messages will not go public.

3. METHODOLOGY

The survey was based on random samples (N=4 001) of Finns aged 18 to 84 gathered from the Finnish population register database. The final data with a total of 1 648 respondents represent the Finnish population relatively well, but as is typical in survey research, there were age and gender related biases. In order to correct for these biases, the data were weighted to meet the age and gender distribution of the Finnish population aged 18 to 84 years. As this study focuses on web-based messaging services, we have excluded the respondents who did not use the Internet at all from the analysis. Thus, our sample consists of 1452 respondents representing 88 percent of the total population which is exactly the same share as that of 16-89-year-old Internet users according to the most recent statistics (OSF 2017).

We use a variable elicited from the question "I worry that my personal messages will be revealed publicly without my consent" as a dependent variable. Answer options were given as a five point Likert scale from 1 "Totally disagree" to 5 "Totally agree". At the beginning of the analysis, we turned the initial scale to measure how confident users are that their private message is kept in secrecy. In the multivariable analyses, we focused on those having high trust by transforming the variable into a binary by recoding the initial values into two categories as follows: 0 was given to those having either low or medium confidence (1 through 3 on the scale) and 1 was given those having high confidence (4 through 5 on the scale).

Our main independent variables are social and institutional trust, which were both combined from three single variables. Social trust was asked with the similar kind of questions used in European Social Surveys: "Most people can be trusted", "Most of the time people are helpful" and "Most people try to be fair". Institutional trust was based on respondents' trust in the parliament, trust in the legal system and trust in the police. Regarding both trust dimensions, respondents were asked to report how much they personally trust each of the institutions or how much they trust other people with a score of 1-5. In this sense, as we use mean variables instead of sum variables, 1 means respondents do not trust at all, and 5 means they have complete trust.

Our control variables included gender, age, education, domicile and Internet use frequencies. Age was measured in years and included as a continuous variable in the analysis. Education was recoded into four categories according to the ISCED classification. Residential area was used by following the NUTS 2 categorization to control the regional level effects. Finally, we controlled for respondents' subjective assessments of Internet and social media use frequency by standardizing on whether the user uses the Internet and social media several hours a day, daily or not more often than weekly. A descriptive overview of applied variables is shown in the Table 1. Mean and standard deviations are calculated only for internet users who had valid scores on dependent variable.

Table 1. Descriptive statistics for dependent and independent variables

	Obs.	Mean	Std. Dev.	Min	Max
Depdendent Variable					
Confidence	1,393	3,0	1,3	1	5
Independent variabels					
Institutional trust	1,392	3,6	0,8	1	5
Social trust	1,380	3,6	0,7	1	5
Controllers					
Gender	1,393	1,5	0,5	1	2
Age	1,393	45,7	16,2	18	83
Education (4 cat.)	1,393	2,6	0,9	1	4
Residence (4 cat.)	1,346	2,5	1,2	1	5
Internet use frequency (3 cat.)	1,393	2,2	0,7	1	3
Social media use frequency (3 cat.)	1,387	1,6	0,7	1	3

In order to determine the extent to which social and institutional trust predict high confidence in private messaging, we used logit models in addition to descriptive methods. For the sake of clarity, we post-estimated the logit models and presented the main results as predicted probabilities. In the body text, we also present the most significant differences as average partial effects with statistical significances.

In addition, we conducted multivariable models to find the extent to which different factors explain the effects of social and institutional trust. For example, social trust may have a significant effect on the level of confidence but the effect can also be due to the level of institutional trust or education. In order to perform a robust comparison between nested logit models, we used the KHB-method developed by Karlson, Holm, and Breen (2012).

The KHB-method provides us with detailed information concerning the mediating effect of intermediary variables. It decomposes the effect of the independent variables into total, direct and indirect effects. The total effect refers to unadjusted effect of the independent variable. The direct effect refers to the adjusted effect that remains prominent when intermediary variables have been taken into account. Finally, the indirect effect describes the share which intermediary variables mediate from the total effect. The results of KHB were estimated as logit coefficients. We present the main results of each analysis in easily interpretable figures by utilizing the user-written packages developed in the Stata program (Jann, 2014; Bischoff, 2017).

4. RESULTS

We began the analysis by defining how confident Internet users are generally that their confidential and private message are kept secret. The results of analysis are shown in the Figure 1. We can see that confidence is distributed quite evenly throughout the population. Approximately 35 percent of Finnish citizens reported low confidence or none at all. A slightly higher proportion (39 %) of respondents reported being highly or completely confident.

An evenly distributed variable gives us a prolific starting point from which to conduct multivariable analysis. As noted before, we estimated the extent to which social and institutional trust predict high confidence by combining those who reported themselves as high and completely confident. As seen in Figure 2, the likelihood of confidence increased significantly according to the level of both trust dimensions. The average partial effect of social trust was 7.8 percent ($p<0.001$) and the detailed analysis revealed that the difference between the lowest and the highest deciles was approximately 19.7 percentage points ($p<0.001$). Interestingly, the effect of institutional trust was not equally strong when compared to social trust. The average partial effect of institutional trust was 6.1 percent ($p<0.01$) as the marginal effect between the lowest and the highest deciles was 15.1 percentage points ($p<0.01$).

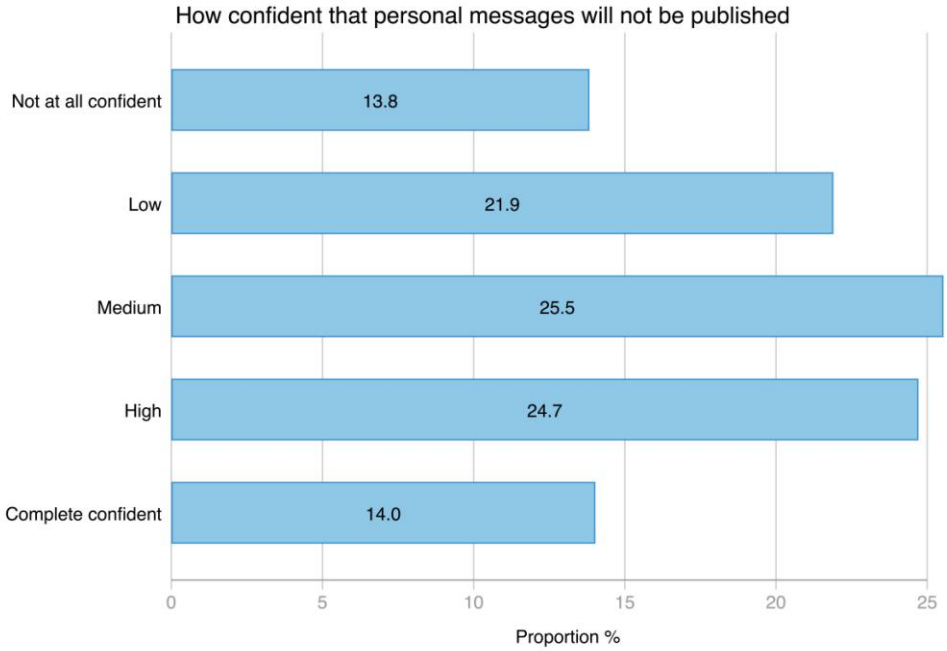

Figure 1. Finnish Internet users' confidence in that their private messages are kept in secrecy, proportions

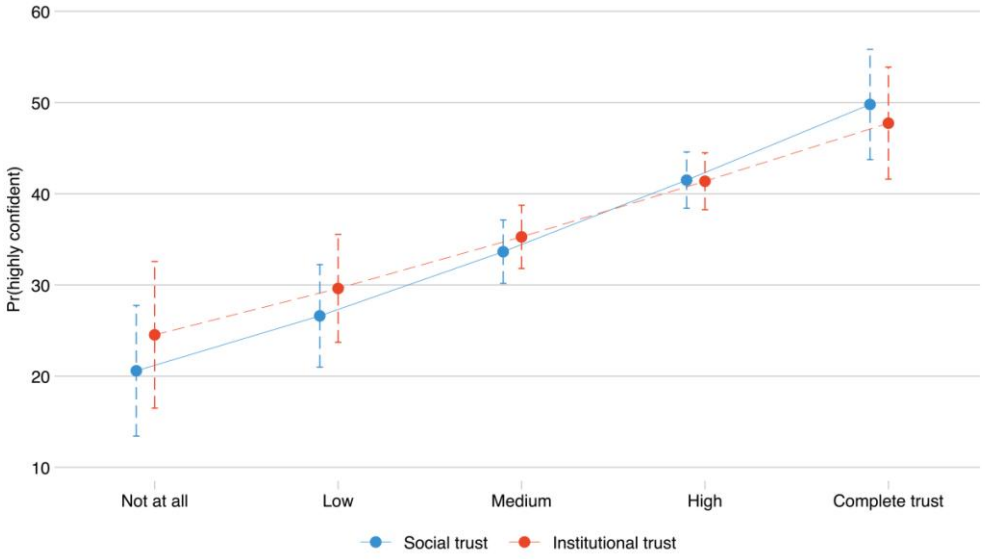

Figure 2. Predicting high confidence in up-keeping of the secrecy of private messages according to social and institutional trust, logit estimated probabilities

We began the next section by assessing the association between demographic factors and confidence. The results of the analysis are presented in Figure 3. Notably, in contrast to our assumptions, the effects of demographic factors were extremely weak. However, according to findings, confidence was to some extent dependent on gender and age, since men and younger participants were more likely to be confident in their message privacy. Interestingly, education and domicile do not have any significant effect on confidence. Instead, those using the Internet several times a day (i.e. hourly) were more confident when compared those using only on a daily or weekly basis. Instead, frequency of social media use had no significant association with confidence.

After descriptive analysis, we also tested whether demographic factors mediate or confound the association revealed in Figure 2 by decomposing the effect between both forms of trust according demographic factors. First, the interplay between trust and confidence of private messages was not explained or mediated by demographic factors. As a matter of fact, we found only one significant indirect effect between age and institutional trust. The detailed analysis of this association revealed that age did not mediate the effect of institutional trust, but rather it strengthened it.

In the final section of analysis, we tested the extent to which social and / or institutional trust mediated one another's effects. The most striking result here was that it was social trust that weakened the impact of institutional trust. Institutional trust did not weaken the impact of social trust. This was confirmed according to the indirect effects presented on the right-most columns of each figure. Here, we can see that the effect of institutional trust was insignificant ($b=0.064$; $p=0.054$) with regard to the effect of social trust, whereas social trust positively promoted ($b=0.102$; $p<0.01$) the effect of institutional trust. According to the detailed analysis of decomposition, social trust explained almost 38 percent of the institutional trust impact. However, only 19 percent of the impact of social trust was explained by institutional trust.

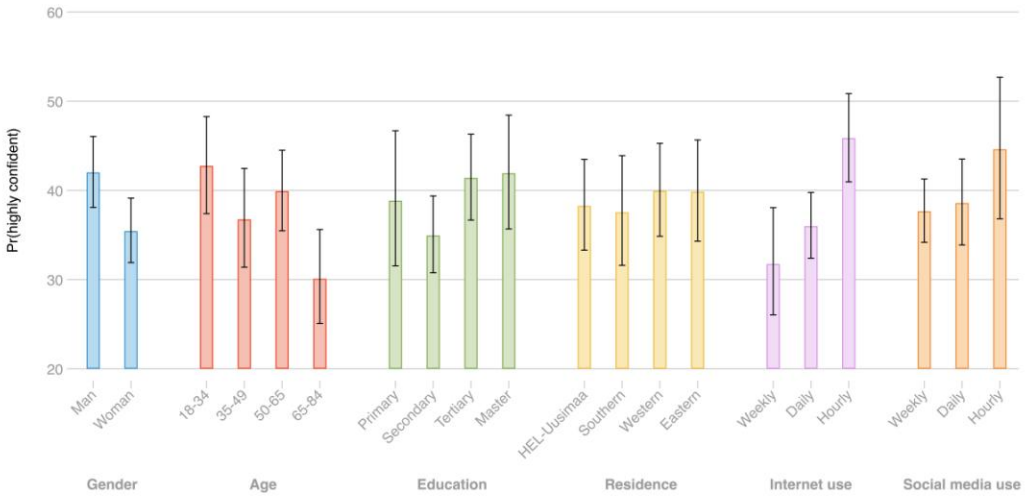

Figure 3. The effects of demographic factors on the high confidence in up-keeping of the secrecy of private messages. Unadjusted predicted probabilities

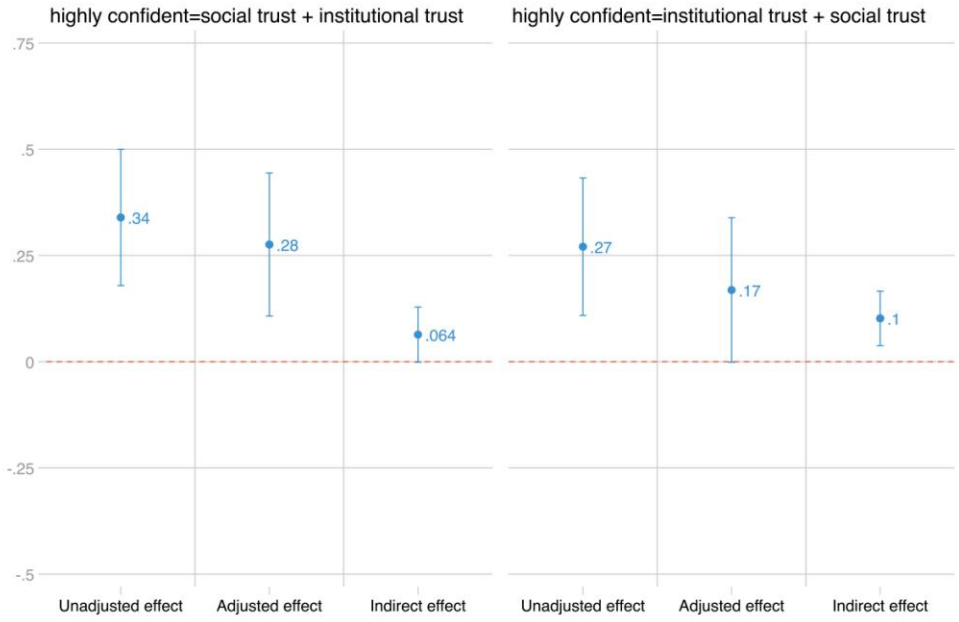

Figure 4. The effect of social and institutional trust on the high confidence in up-keeping of the secrecy of private messages. Decomposed (KHB) logit coefficients

5. CONCLUSION

In this study, our goal was to determine how trusting the users of digital messaging and communication services are in relation to privacy expectations, i.e. how confident users are that their private messages are kept confidential. These results can help us to understand aspects of social and confidential communication in the dynamic and quickly changing digital environment. First of all, it was shown that confidentiality divides evenly at the population-level. We found that a significant proportion of the respondents expressed high confidence, but also a remarkable proportion reported low confidence.

Initially we expected to be able to explain a dividing of confidence through demographic variables. In this respect, we need to emphasize that it was surprising that the extent of user confidence could not be explained by factors of demographic background or Internet access. Instead, high estimates of social and institutional trust form a favorable basis for having high trust in the protection of private messages, i.e. the belief that private messages will stay private. Our results merged with descriptive findings give us the confidence to put forth a conclusion that either trust in the security of private messaging or the revealed effects of social and institutional trust were not explained by the demographic factors of citizens.

Our results are in line with earlier literature, which suggests that there is a close interplay between different forms of trust (Lewis and Weigert, 1985, 972; Kouvo, 2014). Those who trust other people in a generalized manner have high levels of trust towards institutions as well. This is especially the case in Finland and other Nordic countries. However, our results show that social trust is in a more important position compared to institutionalized trust. This may indicate that people are primarily more worried about actions of other users – the receivers – when considering the security of their confidential content. Slightly simplified, an individual who does not trust other people will not trust them online either.

When it comes to institutional trust, we need to bear our mind that in some other countries, institutions are less trusted than in Finland. This may mean that when institutional trust is comparatively high on a national scale, different risks are more likely to be recognized at an individual level. Accordingly, the significance of social trust may be addressed to high institutional trust at an aggregate level. In other words, reliable public institutions enable individuals to have more freedom to act online, and therefore risks and concerns are also strongly related to the dynamics between individuals.

To confirm this assumption, it would be reasonable to continue this study by comparing results from Finland with countries having a lower aggregate-level of institutional trust. In addition, our results should also be tested in other countries where institutions are perceived as equally trustworthy as in Finland.

In simple terms, it seems that if a respondent generally trusts other people, the technical devices in between do not diminish the level of that trust. In such cases, the message is expected to be kept in secrecy and the communicational and technological actors are trusted as well. In a sense, technology becomes invisible because it requires no attention in terms of trust. The applied individual frame, which tells what is happening, is not in an alert mode but is in "this is normal mode". When technology works as expected, it hides its complexity. This means that in terms of the conventional sender-channel- receiver model (e.g. Shannon, 2001), overarching trust between sender and receiver inspires trust in the channel as well. Paradoxically, for trusting users, other users make feelings of privacy possible. However, if a respondent does not trust other people generally, then the technological ways of

communicating become suspicious. The applied individual frame is in the alert mode that hinders communication. In fact, in such a case, privacy comes to designate muteness, silence, and non-communication. In terms of life quality, being constantly suspicious is a wearisome task. Everything raises doubts – both other people and technology.

Overall, it seems that trust remains an essential function in the use of communication technology and services. Different aspects of trust have truly important meaning for companies providing these services. If users don't trust other users, they choose to be silent. If users don't trust the platform or the safety of the platform, they take control of their actions and hinder communication. Interestingly, our results show that trust doesn't depend just on platform features, but wider types of societal trust have important meaning in terms of how people feel privacy risks relate to protection of the secrecy of their private messages. While data breaches, such as in the cases of Facebook/Cambridge Analytica and Ashley Madison, make risks visible and are harmful for both users and platforms, there are wider currents on a societal level, which are shaping experiences of risks and feeling of trust. In this sense, it would be important for future research to assess how different platforms' reliability and various levels of trust are channeling the use and avoidance of different communication platforms and services. It should also be noted that our data focuses exclusive on Finland and therefore these findings cannot be generalized internationally. Also, because trust in its different forms remains a highly important factor in all fields of society, it is important to research the more nuanced associations between trust and different aspects of digital media.

ACKNOWLEDGEMENT

This research was partly supported by the Strategic Research Council of the Academy of Finland (decision number 314250).

REFERENCES

Bischof, D., 2017. New Graphics Schemes for Stata: Plotplain & Plottig. *Stata Journal*, Vol. 17, No. 3, pp 748–759.

Bjørnskov, C., 2012. How does social trust affect economic growth? *Southern Economic Journal*, Vol. 78, No. 4, pp 1346–1368.

Blomqvist, K., 1997. The many faces of trust. *Scandinavian journal of management* Vol. 13, No. 3, pp 271–286.

Coleman, J. S., 1988. Social capital in the creation of human capital. *American Journal of Sociology*, Vol. 94, pp 95–120.

Confessore, N. 2018. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. *The New York Times*. 4.4.2018. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Dewey, C. 2016. It's been six months since the Ashley Madison hack. Has anything changed?. *The Washington Post*. 15.1.2016. https://www.washingtonpost.com/news/the-intersect/wp/2016/01/15/its-been-six-months-since-the-ashley-madison-hack-has-anything-changed/?noredirect=on&utm_term=.417c4ae6620b

Dinesen, P. T. and Sønderskov, K. M., 2015. Ethnic diversity and social trust: Evidence from the micro-context. *American Sociological Review*, Vol. 80, No. 3, pp 550-573.

Ellison, N. B., 2007. Social network sites: Definition, history, and scholarship, *Journal of computer-mediated Communication*, Vol. 13, No. 1, pp. 210–230.

Ermisch, J. et al, 2009. Measuring people's trust. *Journal of the Royal Statistical Society: Series A (Statistics in Society*), Vol. 172, No. 4, pp 749-769.

Freitag, M., and Traunmüller, R., 2009. Spheres of trust: An empirical analysis of the foundations of particularised and generalised trust. *European Journal of Political Research*, Vol. 48, No. 6, pp 782–803.

Garfinkel, H., 1967. *Studies in Ethnomethodology*. Prentice-Hall, Englewood Cliffs, New Jersey. Goffman, E. 1986. *Frame analysis: an essay on the organization of experience*. Northeastern University Press, Boston.

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

Hargittai, E. 2010. Digital na(t)ives? Variation in internet skills and uses among members of the "net generation". *Sociological inquiry*, Vol. 80, No, 1, pp 92-113.

Helliwell, J. F. and Putnam, R. D., 2007. Education and social capital. *Eastern Economic Journal*, Vol. 33, No.1, pp 1-19.

Inglehart, R., 1999. Trust, well-being and democracy. *In Democracy and trust*, ed. Mark E. Warren, 88–120. Cambridge University Press, Cambridge.

Jann, B., 2014. Plotting Regression Coefficients and Other Estimates in Stata. *The Stata Journal*, Vol. 14, No. 4, pp 708–737.

Juntunen, L. and Väliverronen, E. 2010. Politics of sexting: Re-negotiating the boundaries of private and public in political journalism. *Journalism Studies*, Vol. 11, No. 6, pp 817-831.

Kang, C. andFrenkel, S. 2018. Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users. The New York Times. 4.4.2018. https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html

Karlson, K. B. et al, 2012. Comparing regression coefficients between same-sample nested models using logit and probit: A new method. *Sociological Methodology*, Vol. 42, No. 1, pp 286-313.

Keipi, T. et al, 2018. Assessing the social media landscape: Online relational use-purposes and life satisfaction among Finns. *First Monday*, Vol. 23, No. 1.

Kouvo, A., 2014. *Luottamuksen lähteet. Vertaileva tutkimus yleistynyttä luottamusta synnyttävistä mekanismeista*. Sarja C 381. University of Turku, Turku.

Latour, B., 2005. *Reassembling the social: an introduction to actor-network-theory*. Oxford University Press, Oxford.

Lewis, J. D. and Weigert, A., 1985. Trust as a social reality. *Social forces*, Vol. 63, No. 4, pp 967-985.

Listhaug, O. and Ringdal, K. 2008. Trust in political institutions. In Ervasti, H. et al (eds.), *Nordic social attitudes in a European perspective*, pp 131-151. Edgar Elgar Publishing, Cheltenham, UK.

Luhmann, N., 1995. *Social systems.* Stanford University Press., Stanford California.

Mayer, R. C. et al, 1995. An integrative model of organizational trust. *Academy of management review*, Vol. 20, No. 3, pp 709–734.

McEvily, B. et al, 2003. Trust as an organizing principle, *Organization science*, Vol. 14, No. 1, pp 91–103.

Möllering, G., 2006. *Trust: Reason, routine, reflexivity*. Elsevier, Oxford.

Nannestad, P. et al, 2014. Do institutions or culture determine the level of social trust? The natural experiment of migration from non-western to western countries. *Journal of Ethnic and Migration Studies*, Vol. 40, No. 4, pp 544–565

Official Statistics of Finland [OSF], 2018. Use of information and communications technology by individuals [e-publication]. ISSN=2341-8710. Helsinki: Statistics Finland [referred: 2.3.2018]. Access method: http://www.stat.fi/til/sutivi/index_en.html

Rohrschneider, R. and Schmitt-Beck, R., 2002. Trust in democratic institutions in Germany: Theory and evidence ten years after unification. *German Politics*, Vol. 11No. 3, pp 35-58.

Rothstein, B., and Stolle, D. 2002. How political institutions create and destroy social capital: An institutional theory of generalized trust. In *delivery at the Annual Meeting of the American Political Science Association*, Boston, August-September.

Rothstein, B., and Stolle, D., 2008. The state and social capital: An institutional theory of generalized trust. *Comparative Politics*, Vol. 40, No.4, pp 441–459.

Rothstein, B. and Uslaner, E. M., 2005. All for all: Equality, corruption, and social trust. *World politics*, Vol. 58, No. 1, pp 41-72.

Rousseau, D. M. et al, 1998. Not so different after all: A cross-discipline view of trust. *Academy of management review*, Vol. 23, No. 3, pp 393–404.

Schradie, J., 2011. The digital production gap: The digital divide and Web 2.0 collide. *Poetics*, 39(2), 145-168.

Shannon, C. E., 2001. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, Vol. 5, No. 1, pp 3–55.

Solon, O. 2017. Facebook asks users for nude photos in project to combat 'revenge porn. *The Guardian*. 7.11.2017. Available at <https://www.theguardian.com/technology/2017/nov/07/facebook-revenge-porn-nude-photos>

Stroud, S. R., 2014. The dark side of the online self: A pragmatist critique of the growing plague of revenge porn. *Journal of Mass Media Ethics*, Vol. 29, No. 3, pp 168-183.

Subramanian, S. V. et al, 2002. Social trust and self-rated health in US communities: a multilevel analysis. *Journal of Urban Health*, Vol. 79, No. 1, pp S21-S34.

Sztompka, P., 1999. *Trust: A sociological theory*. Cambridge University Press.

Tynan, D., 2016. Facebook's journey ‘only 1% done’ after surge in revenue, Zuckerberg says. *The Guardian* (27.7.2016) https://www.theguardian.com/technology/2016/jul/27/facebook-ad-sales-growth-quarterly-results

Van Deursen, A., and Van Dijk, J., 2011. Internet skills and the digital divide. *New media & society*, Vol 13, No. 6, pp 893-911.

Van Dijk, J.A., 2005. *The Deepening Divide*. Sage Publications, London.

Victor, D. 2015. The Ashley Madison Data Dump, Explained. *The New York Times*. 19.8.2015. https://www.nytimes.com/2015/08/20/technology/the-ashley-madison-data-dump-explained.html

Vuorinen, J. and Tetri, P., 2012. The Order Machine - The Ontology of Information Security. *Journal of the Association for Information Systems*, Vol. 13, No. 9, pp 695–713.

Young, A. L. and Quan-Haase, A., 2013. Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, Vol. 16, No. 4, pp 479-500.