# The Role of Institutional Trust in Estonians' Privacy Concerns

Maris Männiste* & Anu Masso

## Abstract

In this study, we attempted to contribute to previous discussions of the importance of emerging novel data sources in shaping new forms of inequalities and trust culture related to perceived privacy concerns. Our study was based on a representative survey data collected in Estonia in 2014 (n=1503). Two underlying dimensions of privacy were revealed in the analysis: (1) perceived dangers to personal privacy and, (2) perceived dangers to institutional privacy. The analysis of associations only partially confirms the assumption of structural differences in privacy concerns, social groups being somewhat more divided regarding their concerns about institutional rather than personal privacy. Groups more concerned about regarding privacy issues had more frequent social media use as well as higher social activity. The analysis also showed that trust in institutions was related to privacy concerns of different groups and may be one of the key variables explaining the adoption of new technology in Estonia. Thus, besides new structural inequalities related to data practices online, new forms of data activisms are about to emerge, based on perceptions of personal and institutional privacy.

**Key words:** privacy concerns, individual privacy, institutional privacy, trust in institutions, data inequalities.

## Introduction

Digital technologies have become the backbone of most organisational processes and much of what we know about people, organisations, and societies, involves digital sources and activities. Furthermore, new possibilities of measurement, production and governance have become accessible thanks to big data and have led to the social datafication of everyday life (McCosker, 2017). Although the process of 'datafication' has the potential to offer new opportunities and benefits, some authors (e.g. Kennedy et al., 2015) argue that it has also led to new and opaque regimes of population management, control, discrimination and exclusion, and has thereby helped to heighten people's privacy concerns. As consequence, data privacy and security (Pybus et al., 2016), as well as the transparency with which big data companies collect information (Flyverbom et al., 2017), have become major topics of concern in the post-Snowden era. Those issues not only affect the private sector companies anymore, but also governments, which have gained substantial opportunities for the surveillance of communications, movements behavioural patterns, and political activities of citizens (Flyverbom et al., 2017). Although this surveillance has been acknowledged in the context of opressive regimes (Noble, 2018), such practices have now become part of the new normality for most governments, even in liberal democracies (Flyverbom et al., 2017).

It has also been stated that understanding individuals' privacy concerns and behaviour is fundamental to the success of emerging digital technologies (Pavlou, 2011) but in the light of different data leaks, several societies have had to deal with decreasing trust in government services. Also, big data surveillance brings up issues not just of privacy, but also of social sorting and preemption (Lyon, 2014), which have significant implications for people's lives and for the society in general. One good example is the travel restrictions imposed by Donald Trump in the U.S which forbid citizens from specific countries to enter U.S. Although there are problems with immigration and this arrangement may seem to provide a solution, it also fosters inequalities too.

* E-mail address of the corresponding author: maris.manniste@ut.ee

Although we would assume that this have made individuals more aware and sensitive about their data privacy, in many cases they tend to think as one of the Canadian informants in Best's (2010:19) study stated: "Why bother filling my head with this worry when there is nothing I'm gonna be able to do about it, aside from – obviously – pulling myself out from all these things, which you can't really do." Several Eurobarometer studies (e.g. European Commission, 2011, and European Commission, 2016) have also shown similar results regarding Estonians, who seem to be, according to the Eurobarometer study conducted in 2011, one of the most trusting nations in the EU in relation to private personal data and how they are used (European Commission, 2011). Also, according to the later Eurobarometer (2015) study, the majority of Estonians tend to agree with the statement "I do not have anything to hide" (74%) and seem to agree with the fact that gathering data is inevitable and people just have to come to terms with it (European Commission, 2015). Still, as Estonia as the '*most advanced digital society*' (Hammersley, 2017), relies more and more on personal information posted and shared voluntarily by the users of various e-services, issues related to privacy have become more important. In fact, the need to conduct everyday online transactions has led to the fact that Estonians have become very accustomed to sharing and seeking personal information online. Although Beldad et al. (2010) emphasise that it has been stressed that trust is crucial in the adoption of e-government services, there are still very few available studies in this area, compared to the sizeable number of similar studies of e-commerce (Beldad et al., 2010), and this makes Estonia interesting sample case to be studied from several aspects.

In this article, we strive to contribute to previous studies explaining people's concerns regarding privacy. Although the theoretical literature has paid a lot of attention to the importance of emerging novel data sources in shaping new forms of inequalities, little quantitative empirical research has focused on the issues. Studies have indicated that online experiences, related to access and autonomy are structured in terms of differences in social status (e.g. Hargittai, 2008; Park, 2013; Robinson, 2009; Smith et al., 2015). Some authors emphasise that privacy concerns can be explained by socio-demographic characteristics, e.g. age (Van den Broeck et al., 2015; Kezer et al., 2016), users' educational background (Park, 2013), technical familiarity (Litt, 2013), or privacy literacy skills (Bartsch & Dienlin, 2016), while others find that being vigilant about privacy is only the outer layer of digital nested habits (Büchi et al., 2017). In this article we study the privacy concerns in Estonia in the context of socio-demographics and status differences and analyse variations in privacy concerns regarding perceived violations of individual and institutional privacy and relationships with the general institutional trust culture. Estonia, as a post-Soviet country, can be seen as a good example of a country where one would assume that previous regimes have made individuals distrustful but, as studies indicate (Beilmann & Realo, 2018), trust in the last 20 years has been instead increased in Estonia and, regarding trust in different governmental institutions (e.g. the police, the legal system) (Roots et al., 2016), it has been noted that level of trust is almost the same as in the older democratic states of Europe.

## Theoretical overview

### *Online privacy concerns*

Research (e.g. Baruh & Popescu, 2015; Hull, 2015) indicates that people still see privacy as an important value, but as technological advances have made personal data gathering and sharing often invisible (Acquisti et al., 2015), individuals often do not have complete knowledge about what, why and for which purposes data is collected about them and how this data is used. Furthermore, although a user can be careful about what information is posted, outside access can also result in privacy violations and harm (Joinson et al., 2011). Thus, in the context of this article, we understand privacy not as solely about individual pieces of personal information that the individual wishes to control i.e. in the context of personal or individual privacy, but as also concerning the practices of sorting and classifying individuals for specific purposes (Mai, 2016) i.e. related to institutional privacy. In addition to social and institutional privacy, we must consider that privacy is a dialectic process wherein individuals seek a balance between openness and closed-ness in relation to specific persons, groups, or organisations at a given time (Archer et al., 2015) and privacy can also be contextual depending on certain situations – especially when we are talking about different social media sites or other digital platforms. Raynes-Goldie (2010) differentiates between social and institutional privacy. Social privacy refers to situations where other, often familiar, individuals are involved. Receiving an inappropriate friend request or being stalked by a colleague are examples of social privacy violations. Institutional privacy, in contrast, describes how institutions (such as Facebook, as in Raynes-Goldie, 2010) deal with personal data and is related to users losing control of the collection and processing of their information (Gürses & Diaz, 2013:30). As social privacy is more about users' behaviour, this kind of privacy assurances tends to be more understandable and accessible to users.

Still, there is a connection between institutional privacy, individual privacy and institutional privacy assurances (Xu et al., 2011). For example, institutional privacy assurances, such as privacy policies, can reduce individual privacy concerns. This has been confirmed in Talebi et al.'s. (2017) study, which showed that privacy assurance statements affect privacy concerns positively. One possible factor is that users must perceive the privacy statement as adequate to feel that their privacy is protected, otherwise not only does it not reduce privacy concerns, it increases users' concerns regarding their privacy. While several authors have indicated that privacy policies should reduce privacy concerns, users indicate that privacy policies are too long, too hard to understand and for that reason they tend to ignore them (Gluck et al., 2016; Smith, 2014; Anthes, 2015). This may be one of the reasons why several studies of social network sites have indicated that users (particularly younger users) are more concerned with their social privacy than their institutional privacy (Raynes-Goldie, 2010; Young & Quan-Haase, 2013).

Also, as Xu et al. (2008) showed, the role of the service providers in e-commerce is perceived differently by their users in comparison with social media. For example, security measures in e-commerce sites are expected by their users and lead to lower perceived levels of privacy risk. The situation is reversed in social media settings, which highlights the role of social networking providers in the assurance of safe personal information handling.

Additionally, privacy concerns, or the worries and concerns people have about the accessibility and control of their personal information, are influenced by culture and norms (Petronio, 2002) and vary across a host of micro and macro level factors such as age, gender, education, Internet experience, nationality and cultural values (Hichang, 2009). These concerns can also be affected by a number of personality traits (Bansal, 2016). Although, some studies show that women are more concerned about others accessing their personal information (Tufekci, 2008; Hoy & Milne, 2010) and female adolescents tend to protect their online privacy better by disclosing less information and instituting more access restrictions on their online profiles (Walgrave et al., 2012), there are also studies which indicate that men are better equipped with privacy technical aids and that higher confidence in privacy protection is associated with being male (Park, 2015).

It has also been noted by some authors (e.g. Courtney et al., 2008; Kezer et al., 2016) that most of the empirical research so far has mainly focussed on online privacy as experienced by teenagers and young adults (e. g Livingstone et al., 2011; Dhir et al., 2016; Walrave et al., 2012). This tendency to focus on youth is likely related to them being the first and most enthusiastic users of the Internet. Also, while younger users are typically more active and skilful (Bridges et al., 2012; Dahlgren, 2011) older Internet users use lower levels of privacy protection and they are also less skilled (Büchi et al., 2017), yet skills remain the strongest predictor of privacy protection as users need general skills in navigating the Internet to apply self-measures in their everyday Internet use (Hichang, 2009; Ellison et al., 2011, boyd & Hargittai, 2010). Besides skills, the effect of age on Internet and online engagement can also be related to the users' interest (Blank & Lutz, 2016), for example older users may be more interested in specific topics like politics or health in Internet.

To the contrary, the Taddicken study (2013), which researched German Internet users' privacy concerns, found that age had little connection to social media information disclosure, or privacy concerns. Similarly, based on representative U.S. sample, Hoofnagle et al. (2010) found no significant differences related to age across a range of privacy variables. To understand generational differences, Miltgen and Peyrat-Guillard (2014) conducted focus groups with young people (14-24) and adults (25-70) in seven European countries, including in Estonia. Their study (Miltgen & Peyrat-Gullard, 2014) indicated that middle-aged respondents (45-60 years old) perceived more privacy risks online and had greater fear regarding privacy invasion compared to younger people.

Blank & Lutz (2016) also indicate that there is a positive correlation between education and possible harms and benefits users encounter online. One would assume that education would equip users with better coping strategies, but the findings of Blank and Groselj's study (2014) show that, as educated users tend to use a wide variety of applications (e-banking, online-shopping etc.), they are also more likely to experience risks online. Furthermore, educated users may also be more experimental in their surfing behaviour which can also expose them to greater risks (Blank & Lutz, 2016). Studies have demonstrated that concerns about online privacy vary across a host of individual factors. More specifically, the literature suggests that gender, age and education may be the significant factors affecting online privacy concerns. Consequently, this study hypothesizes as follows:

**H1:** Awareness of possible privacy violations and perceived privacy concerns is unequally distributed across socio-demographic groups, so that higher privacy concerns are negatively associated with age and positively associated with social status differences (e.g. education and social level).

Additionally, possible different socio-demographic and status differences, Debatin et al. (2009) found also that a person who experienced a "privacy invasion" on Facebook (such as public humiliation from another member) was more likely to adjust his or her privacy settings than someone who had only heard about such occurrences but had not experienced them personally. Several studies have confirmed that, besides Internet skills, changes in (social media) privacy settings and Internet use frequency (boyd & Hargittai, 2010; Blank & Lutz, 2018), technical familiarity (Park, 2013; Blank & Lutz, 2018) has an impact on individuals' privacy strategies.

There is also evidence that highly active users are not more or less sensitive about their personal information than low-use individuals, but since they are more likely to encounter privacy threats, they have developed strategies to manage their online privacy – contingent upon their skills in doing so (Büchi et al., 2017). But as Blank and Lutz (2018) argue, individuals who experience such problems as viruses, misrepresented goods, or credit card theft, may simply regard those problems as a cost of being on the Internet. For those people, the benefits may outweigh the risks. This was seen in Ostherr et al.'s study, in which respondents felt little concern about sharing their user-generated health data with corporations. This may be related to the fact that the transactional nature of their consent overrode any concern about privacy and the fact that individuals had already decided that they wanted to use a device or piece of software, so they consented to the terms of use in exchange for access to the product they desired. Turow et al. (2015) have called this "the trade-off fallacy", noting that most Americans feel it is impossible to limit access to their data, and instead see digital profiling as inevitable. Still, although some may say it is inevitable, profiling and sharing their customers' data affects trust related to certain services and future behaviours regarding privacy. Hoffman et al. (2016) have also proposed the term 'privacy cynicism' which means that users take advantage online services without trusting providers but are aware of privacy threats and therefore have an opinion that privacy protection is out of their hand. Also, repeated consumer data breaches have given people a sense of futility, which have ultimately made them weary of having to think about online privacy, as Choi et al. (2017) emphasise referring to this phenomenon as 'privacy fatigue'.

As indicated in the TRUST e-privacy index (2014), 89% of British consumers avoided doing business with companies they did not believe protected their online privacy. There is a clear philosophical distinction between how Americans treat their personal data compared to Europeans: Americans perceive their personal data to have economic value. A recent study (Marwick & Hargittai, 2018) indicated that people make privacy decisions in which they carefully weigh the costs and benefits of providing personal information to institutions such as governments and corporations.

Financial benefits, health benefits, convenience and necessity are motivators for individuals to choose to use different platforms and e-services and a lack of trust, fears of online harassment and fears of discrimination are the main demotivators for doing it. Focus groups conducted in a study (Marwick & Hargittai, 2018) indicated that users evaluate information type, context and the institution requesting information when choosing whether to share information. Consequently, this study hypothesises as follows:

**H2:** Internet use practices and sharing information about oneself on social media have positive effects on individual privacy concerns.

### *How does trust affect privacy concerns?*

Several studies (e.g. Wakefield, 2013) have shown that one of the determinants of people's tendency to disclose personal information on websites is perceived trust. Corritore et al. (2003) have defined online trust as an attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited. Trust has also been conceptualised as an antecedent (e.g. in Wakefield, 2013) and as an outcome of privacy concerns (e.g. in Bansal et al., 2010), but some (e.g. Anderson & Agarwal, 2011; Dinev & Hart, 2006) argue that trust and privacy concerns are independent factors that may exert separate influences on intentions to disclose information. It has also been noted in some cases that privacy concerns are rather negatively associated with trust (e.g. Kim et al., 2008).

Belanger, Hiller & Smith (2002) have defined trustworthiness as the perception of conviction in the trusted entity's reliability and integrity. Internet users strive to judge the trustworthiness of service providers by considering several trust cues or signals which permit an estimation of service competence, benevolence and integrity (Beldad et al., 2010; Bart et al., 2005). Several authors (e.g. Wright, 2017; Flyverbom, 2017) also emphasise the importance of transparency, which according to Wright (2017) refers to governments and companies informing citizens in ways they can easily understand about surveillance practices, about the presence of surveillance technologies, about who is responsible for surveillance systems, and about why those systems have been deployed.

It is the same in social networks where users must choose how much personal information they want to share and with whom: this in itself is a trust decision where users think about who can be trusted and with what information. This is also supported by the findings of Song, Hao and Daqing's study (2013), where people who had higher trust in social networks were more likely to participate actively in those networks than those who were less trusting.

While in an offline context the object of trust is typically a person or an entity, online, it is the technology (primarily the Internet) and the organization deploying the technology. This means that in the online context customers of electronic commerce not only evaluate the website but also the company behind the site, and even an explanation of why the site is trustworthy (Boyd, 2003) can increase or decrease trust. Thus, it is beneficial for online organisations to improve their reputation, performance and appearance, because it leads to being seen as trustworthy (Beldad et al., 2010).

According to Clarke (2014), trust may arise from a direct relationship between parties (such as a contract, or prior transactions), or from experience (such as a prior transaction, a trial transaction, or vicarious experience). When such relatively strong sources of trust are not available, it may be necessary to rely on "referred trust", such as delegated contractual arrangements, "word-of-mouth", or indicators of reputation (Clarke, 2014; Beldad et al., 2010). Users tend to underestimate the risks of information disclosure when confronted with a user interface that elicits positive emotions (Kehr et al., 2015). Trust can also be influenced either by users' experience with the technology used for transaction or just by their tendency to trust (client-based trust antecedents) (Beldad et al., 2010) or by the quality of the website used for the transaction or the presence of security assurances on the website (web-based trust antecedents) (Beldad et al., 2010). It can also

be affected by the personalisation afforded by the e-commerce site (Xu et al., 2011).
It is evident that several data breaches have affected users trust in governments and private companies and have heightened privacy concerns. This problem is, as Flyverbom (2017) emphasises, not just a result of insufficient security or protection on the part of the companies involved, but of users installing "third-party applications" that are able to tap into their accounts and, as a result, leak their own and others' data. This seems to indicate that in this digital society, specific skills gain more and more importance in maintaining trust in services used, otherwise, problems which have arisen from other users may affect trust on specific institutional entities. Consequently, this study hypothesises as follows:

**H3:** We assume that general trust in institutions decreases the feeling that privacy in online context is being violated, and increases intentions to disclose information on social media, or vice versa, people who feel that institutions violate their privacy online also trust different institutions less.

## Data and Method

This article is based on data from the fifth round of the representative population survey "Me. The World. The Media", carried out by the Institute of Social Studies, University of Tartu, and Saar Poll market research company at the end of 2014. The survey covered the Estonian population 15 to 79 years old, with a total sample size of 1503 (1028 respondents completed the questionnaire in Estonian and 475 in Russian). To alleviate the differences between the representative population model (based on the demographic statistics) and the sampling outcome, the data were weighted by the main socio-demographic attributes (gender, age, ethnicity, and place of residence) (Vihalemm & Masso, 2017). The survey covered attitudes towards changes in Estonia during the past ten years, values, political and civic participation, usage of time, media use, life-styles and life conditions. A self-administered questionnaire, combined with an interview, was used.

In this study, we focused on analysing a group of variables measuring the perceived dangers to privacy. The following question was formulated in the questionnaire: *Have you ever had the feeling, that the following institutions, companies or persons are violating your privacy, by using the Internet or social media?* Then variants were presented to the respondents, who were asked to evaluate them on the five-point frequency scale with 5 being - constantly, very often, 1 being - not at all: state institutions, local governmental institutions, employer, business enterprises, health system, the educational system, foreigners, friends and acquaintances and family members (see Appendix 1, Table 2). To examine the associations between privacy concerns and trust, the following independent variables were used: *various institutions and groups essential in Estonian society are listed. Please choose in each row one variant from one to five that best characterizes the trustworthiness of them for you.* A list of 13 groups or institutions was presented to the respondents, including societal and media institutions and various influence groups. The respondents were asked to evaluate them on at five-point scale, with 5 being - trust completely and, 1- do not trust at all. Based on these single variables, the following composite indexes were calculated: trust in representatives of governmental institutions (including such institutions as parliament, the Estonian state, politicians, the president and officials), trust in other state institutions, trust in media institutions (television and radio channels of Estonian Public Broadcasting, private television and radio channels, newspapers, Facebook and other social media and Internet portals), and trust in cultural and surveillance institutions (schools and educational systems, the health system, the court system, banks, police, cultural activists, scientists, public companies and, churches).

Besides the main dependent variable of privacy concerns and trust in institutions and groups as the main independent variable, we used several socio-demographic control variables in the analysis: gender (1=male; 2=female); ethno-linguistic affiliation (1=Estonian-speakers, 2=Russian-speakers), education (from 1= primary education to 14=higher education with doctoral degree); income (from 1=less than 60 euros to 12=more than 1000 euros per month per household member), self-estimated social status (from 1=low status to 5=high status). Besides socio-demographic control variables, index variables characterising social media use were included in the analysis:

self-expression and communication-centred Internet use (uploading photos and videos online, downloading and sharing music or films, following friends and acquaintances in social media, sharing the information about oneself on social media, speaking up in forums, commenting on articles and sharing media news), use of various social media channels (frequency of using Facebook, Twitter, Snapchat, Instagram or other photo-sharing networks, Foursquare or other location-sharing services, YouTube, LinkedIn, World of Warcraft or other gaming communities and Geni.com), being concerned about mobile or smartphone overuse in the vicinity (being disturbed if mobile and smartphones are used in meetings or at school, at home among family members, on public transport, in cafés, in the cinema, in theatres or at concerts), functional versatility of social media use (sharing information, changing information, asking for support, sharing news, discussing TV/radio programmes, discussing political issues, commenting or asking questions regarding topics related to health and cultural events, suggesting books, films or music, sharing information about products or services, following social media pages, inviting friends to participate in events, and giving feedback to public institutions and giving opinions about products and services). In addition, another calculated index variable, enterprisingness, was used as background control variable. This index variable was calculated by summing the following single variables: (1) *Do you consider yourself an enterprising person?* (2) *What is your relationship with various economic activities? (being an owner of a company or one of the managers of a company, buying or selling a stock, investing money in a foundation), and* (3) *Do you get any additional income from activities other than your main work?* This index variable also reflects the general activity of a person, as well as characterising economic activities.

First, we used principal-component factor analysis with the Varimax rotation technique to reveal underlying relationship patterns among the privacy concerns regarding a list of institutions, groups or individuals. To compare age groups in terms of their privacy concerns, we calculated individual factor scores and analysed the mean scores across age groups. The relationships between the privacy concerns, socio-demographic variables, social media use and perceptions of social trust were explored by using generalised linear regression analysis.

## Results

### *Concerns about privacy*

To determine whether underlying relationship patterns among the statements about privacy concerns referred to the trust in institutions or other individuals, we first used principal component factor-analysis with the Varimax rotation for finding the underlying dimensions of privacy concerns, and then we analysed relationships between these latent dimensions of privacy concerns with trust in institutions. The results in Table 1 reveal clear and interpretable factor structure with two main factors, explaining about 68 per cent of the total variation.

**Table 1:** Factor loadings of the concerns about privacy * **

| Concerns that the following institutions, companies or individuals are violating your privacy... | F 1: Institutional privacy | F 2: Individual privacy | F 1: Total privacy concerns*** |
|---|---|---|---|
| Local governmental institutions | .864 | | .824 |
| State governmental institutions (police, tax board, etc.) | .806 | | .783 |
| Employer | .751 | .343 | .804 |
| Business institutions | .680 | | .662 |
| Educational system | .672 | .463 | .815 |
| Health system | .653 | .456 | .796 |
| Friends and acquaintances | | .885 | .751 |
| Family members | | .854 | .708 |
| Foreigners | .442 | .575 | .702 |

*Notes:*
* Principal component analysis with Varimax rotation.
** Higher loadings in a factor are marked in bold. Factor loadings <.3 are excluded from the table.
*** One-component solution without rotation.
*Source:* authors' calculations, based on data from the survey "Me. The World. The Media".

Factor 1 involves six positive statements focusing mainly on items which referred to privacy violations related to specific institutions, such as like local government or other governmental institutions, employers, commercial enterprises, and educational and health systems. Accordingly, we labelled this factor *Institutional privacy*.

Factor 2 involves three statements focused on privacy violations by friends, acquaintances, family members and foreigners. Based on the content of the main variables, we labelled this factor *Individual privacy*.

Besides these main variables explaining the composition of the factors, four variables are multidimensional (have factor loading higher than .3 in two components, marked in the table with regular font). For comparative purposes the table also includes the factor solution with only one factor (explaining 58 per cent of total variation). Based on Catell and Kaiser's criteria the one-factor solution was suggested since only one factor has eigenvalues >1. However, we also decided to comparatively use a two-factor solution distinguishing two main types of privacy concerns – individual and institutional – as suggested in the literature (Xu et al., 2011; Gürses & Diaz 2013).

We saved the individual factor scores for each component for the next analysis. Also, analysis with Cronbach's Alpha revealed, that the internal consistency of these factors was .8 in the case of individual privacy and .886 in the case of institutional privacy, which is considered as highly reliable (Warner, 2013). Therefore, it is statistically reliable to use these factor variables for further analysis. Next, analysis of variance (ANOVA) was used to compare the average levels of individual privacy concerns, institutional privacy concerns and general privacy concerns among different age groups (Fig. 1).

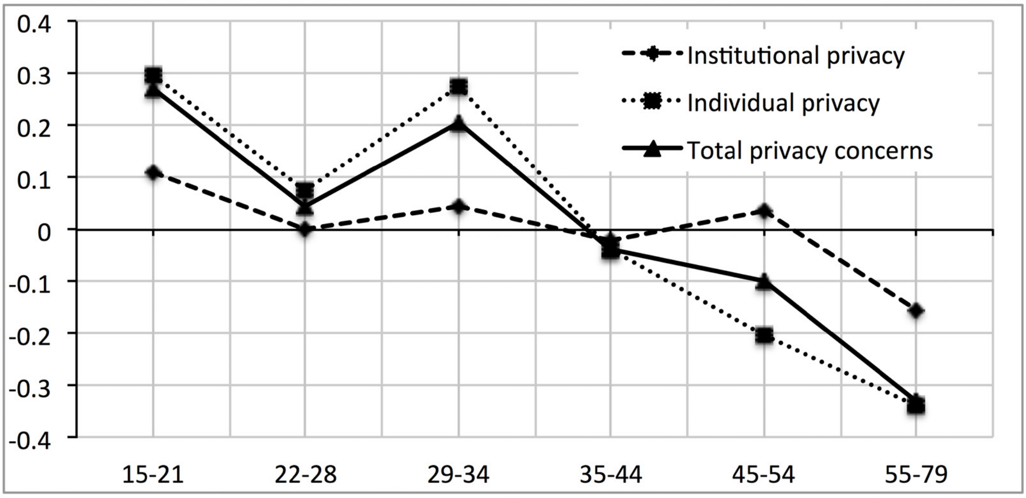
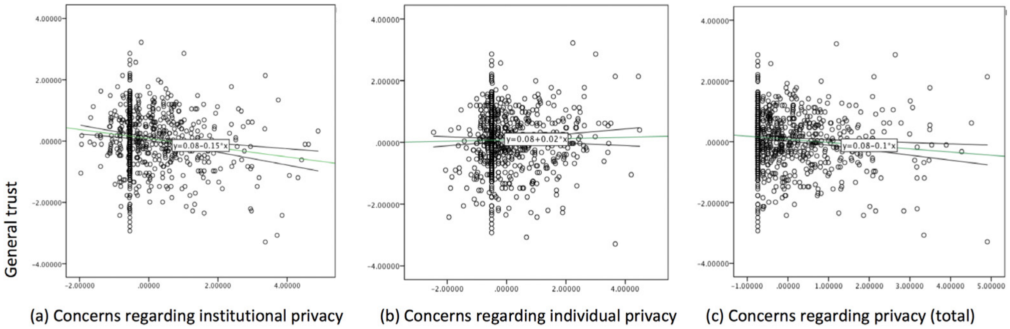


**Figure 1:** Concerns regarding privacy in age groups (mean factor scores)

*Source:* authors' calculations, based on data from the survey "Me. The World. The Media".

Factor 1, *institutional privacy*, from the youngest age group onward fluctuated little bit but remained almost linear until the oldest age group (55-79 -years old) who were visibly less concerned about institutional privacy. For this age group, the concern about *individual privacy* was also the lowest. The age groups 15-21 years old and 29-34 years old were most concerned about individual privacy, while, surprisingly, the age group (22-28 years old) showed less concern about individual privacy. From age 35 and older the concerns about individual privacy linearly decreased and dropped noticeably below the concerns about institutional privacy. All of the analyses showed that differences between age groups were statistically significant only in the case of individual privacy, indicating that younger people tended to be more concerned about their individual or institutional privacy (F=8,5, p<.000).



(a) Concerns regarding institutional privacy
r=-.160**

(b) Concerns regarding individual privacy
r=.023

(c) Concerns regarding privacy (total)
r=-.112**

**Figure 2:** Bivariate associations between general trust in institutions and (a) concerns regarding institutional privacy, and (b) concerns regarding individual privacy (**p<.01)

*Source:* authors' calculations, based on data from the survey "Me. The World. The Media".

Figure 2 shows that there was a relationship between trustworthiness and the perception of privacy concerns, primarily through institutional privacy. The correlation in this part was statistically significant but relatively weak. It is also evident from these results that there was no statistically significant relationship between individual privacy concerns and trustworthiness, indicating that in an online situation trust in different institutional entities is more important and will have more effect on privacy concerns than trust in other people, such as friends, family or foreigners.

### *Predictors of concerns about privacy*

We were intrigued by the fact that two generation groups varied a lot in their concerns about institutional privacy; we decided to analyse the influence of other explanatory variables. We carried out a series of generalised linear regression analyse (GLM) with the factors of concern about privacy as the dependent variables. In addition to age as the main hypothesised predictor, we included other socio-demographic variables and index variables measuring social media use and habits and trust in institutions in the analysis. The goodness of the fit of the regression models were estimated using AIC and Likelihood Ratio Chi-square indicators, both indicating statistically significant and good fits of the models (see the results in Table 3).

The results in Table 3 show that the regression models 1 and 2 differed in some interesting ways indicating that the concerns regarding individual privacy were strongly related to age, while concerns regarding institutional privacy do not have statistically any significant relation to age. While age seemed to be the only socio-demographic variable explaining the variation in individual concerns, there was some variance between gender and education as socio-demographic variables in institutional privacy concerns, which may indicate that women and people who had higher education may have had higher concerns about institutional privacy. The negative regression coefficient related to age shows that older generations were less concerned about individual privacy, which can be related to several factors, e.g. Internet usage frequency or differences in online services used by different generations. The results also indicate that a variable measuring social media use and habits e.g. discomfort with mobile or smartphone usage at close range, was related to both individual and institutional privacy concerns.

Interestingly, there was no statistical significance between frequency of using various social media platforms and individual privacy concerns, but social media usage did explain institutional privacy concerns. Therefore, particular content-related activities rather than pure use of social media channels explained concerns regarding privacy.

It is also notable that there was no statistical significance between trust in different institutions and individual privacy concerns. To the contrary, analysis showed that trust in governmental institutions statistically significantly explained concerns about institutional privacy, i.e. institutions which were perceived to be more trustworthy were also perceived to violate institutional privacy less. The latter finding is important, for example, in the context of the adoption of various e-services and is one of the reasons why Estonians are willing to make such active use of e-services. Trust in media institutions, trust in other state institutions and institutional privacy concerns were statistically significantly associated, indicating that the way people perceive those institutions explains their concerns. As consumer or user profiling is quite common and there have been several well-known data breaches and instances of malpractice (e.g. with LinkedIn and Yahoo.com), people may feel that as the practices different private companies use are mainly unseen and uncontrollable by them, they may be more likely to violate privacy. In addition, an interesting relationship was revealed between institutional privacy concerns with the index variable of enterprisingness, indicating that individuals with higher participation in enterprise-related activities expressed higher levels of concerns regarding institutional privacy.

## Discussion and conclusions

The aims of this research were to contribute to previous discussions about the importance of emerging novel data sources in shaping new forms of inequalities and trust culture related to perceived privacy concerns. In this study we examine concerns regarding privacy, testing the hypothesis raised in previous studies about socio-demographic and status differences in privacy concerns, and variations of privacy concerns related to perceived violations regarding individual and institutional privacy and relationships to the general institutional trust culture. Our study was based on representative survey data collected in Estonia in 2014 (n=1503). Two underlying dimensions of privacy revealed in the analysis were: (1) perceived dangers to personal privacy and (2) perceived dangers to the institutional privacy.

Contrary to some previous studies (e.g. Hoofnagle et al.,2010), the findings of our study revealed that in comparison to older age groups younger people expressed higher individual privacy concerns (H1). Interestingly, regarding institutional privacy concerns, there was less variation between different age groups, indicating that although age inevitably explains younger people's privacy concerns, it does so less for institutional ones. Several other socio-economic variables, such as gender and education which have been mentioned by other authors (e.g. Tufekci, 2008; Hoy & Milne, 2010; Walgrave et al., 2012) also were prominent regarding institutional privacy, indicating that also in Estonia there are differences between how women and men or well-educated people perceive threats to their privacy, although the relationships were rather small.

One dimension which may also explain how different age groups perceived privacy violations was related to previous experiences with certain problems in online context. As Debatin et al. (2009) have indicated, users who are more active in online settings are more likely to encounter privacy violations. Still, our study did not show any significant relationship between different types of Internet use and individual privacy concerns, indicating that those concerns can be related with some other variables (H2). Contrary to individual privacy concerns, institutional privacy concerns were positively related to several different social media uses and habits, indicating that people who used more online environments to create user-generated content or to communicate or take more initiative, were less concerned about institutional privacy. Heightened worries about institutional privacy may also be a result of different globally recognised data breaches, which are mainly related to companies and other institutions rather than to other individuals. Skills as one of the prerequisites explaining privacy concerns have also been noted by several authors (e.g. Hichang, 2009; Ellison et al., 2011; Strater & Lipford, 2008).

Several authors (e.g. Wakefield, 2013) have found that trust is one of the prerequisites that explains privacy concerns. Our analysis showed that trust in governmental institutions was rather strongly associated with institutional privacy concerns (H3). A negative association means that when people have trust in governmental institutions, they are less likely to be concerned about privacy over all. To gain trust and to prevent concerns about surveillance which evidently will affect trust in governmental institutions and the use of different governmental services, several steps have been taken to improve transparency, which means that citizens are well informed about how and for what reasons their government is using surveillance (Wright, 2017). What may have helped increase transparency are cases where government officials (e.g. in the Alice Järvet case) have been brought to justice for unnecessary searches of other people's personal information in government databases. Also, one of the possibilities connected with e-government and different e-services in Estonia is that, citizens themselves can check which institutions have searched for their personal information in governmental databases and they have the right to demand explanations why this was done. This may be one of the reasons why Estonians trust in governmental institutions has been increased in past 20 years (Beilmann & Realo, 2018). Miltgen and Peyrat-Guillard's study (2014), which also included focus-group interview participants, also showed that while data disclosure is a matter of public concern in all other countries in their research (e.g. in Poland and Germany), in Estonia the discussion is more centred on data that can be made public.

Although several legal decisions issued by European Union (e.g. GDPR) will affect how private companies and governmental institutions handle and use data they have gathered, many of the problems will still be present and will lead to the emergence of different data activists. More integration of several different data sources will provide good opportunities to discover patterns which might otherwise go unnoticed or be hard to comprehend in real life, but also foster some new practices which will inevitably violate people's privacy. Those new practices will bring to the forefront more vulnerable groups which are somewhat different in their daily activities or may be somehow problematic for governments (immigrants, people who need social aid etc.). The social sorting from the data gathered will be the main indicator which will affect future decisions made about those people and can lead to new and more complex problems. This may directly affect services which will be provided for them, opportunities they will have and how they will be seen in society. Those are just a few problematic situations which could foster the development of data activism in Estonia.

An interesting relationship revealed in this study was that institutional privacy can be accurately explained by individuals' enterprisingness. Our analysis revealed, that individuals who have had more contacts with various (business) institutions and thus perhaps also more experiences with datafication practices of institutions had developed their individual opinions and experiences regarding privacy concerns related to these institutions. This relationship may also suggest the emergence of certain data activism initiatives of individuals, indicated in several previous studies (see e.g. Dencik et al., 2016) and in the form of citizens' activities, based on experienced privacy concerns. However, as we could not determine the direction of the relationship based on the survey data, additional (semi)experimental studies focusing on privacy concerns of active users of provided private or public institutional services, are needed.

Our results are not without limitations, which offer interesting opportunities for further research in this area. The first limitation involves using data which originates from 2014 and this means that the actual privacy concerns of Estonians may have changed in the last few years due to the rapid digital transformations and the emergence of novel datafication practices and related privacy concerns. Therefore, several topics which may explain people's privacy concerns and trust issues couldn't be analysed as at the time when this survey was carried out those problems were not as prevalent or visible in Estonia. For example, we couldn't analyse the relationship between privacy policies i.e. we were unable to identify a relationship between privacy policies as one of the possible factors fostering trust between institutions or private companies and privacy concerns.

Nevertheless, the results indicate several intriguing factors which may explain how Estonians'perceive privacy violations and why Estonians are so willing to use digital technology. This also indicates that trust in governmental institutions and trust culture in society in general affect the implementations of e-services even more in Estonia than was previously thought. A, future study could research in more depth the specific factors which affect Estonians' trust in certain e-services. Adopting new General Data Protection Rules will also affect both individuals and institutions in many levels and may affect how privacy is perceived even more. As this has been a rather important topic also in Estonia and several institutions will have to change their data practices to offer more privacy-enabling possibilities for individuals, it is also important to gather more data on people's privacy concerns and on which institutions and companies in Estonia they are worried about gathering information about them.

## References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514.

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research, 22*(3), 469-490.

Anthes, G. (2015). Data brokers are watching you. *Communications of the ACM, 58*(1), 28-30.

Archer, K., Christofides, E., Nosko, A., & Wood, E. (2015). Exploring disclosure and privacy in a digital age: Risks and benefits. In L. D. Rosen, N. A. Cheever, & L. M. Carrier (Eds.), *The Wiley handbook of psychology, technology and society* (pp. 301-320). Hoboken, NJ: Wiley-Blackwell.

Bansal, G., Zahedi, F. M., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138-150.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. Information and *Management, 53*(1), 1-21.

Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. *Journal* *of Marketing, 69*(4), 133-152.

Bartsch, M. & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behaviour, 56*, 147-154.

Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management. *New Media & Society, 19*(4), 579–596.

Beilmann, M., & Realo, A. (2018). Õppides usaldama. Üldine usaldus Eestis aastatel 1990-2016. [*Learning to trust. General trust in Estonia between 1990-2016.*] Akadeemia, 30(6), 979-1011.

Belanger, F., Hiller, J.S., & Smith, W.J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems, 11*(3-4), 245-270.

Beldad, A., De Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior, 26*(5), 857-869.

Best, K. (2010). Living in the control society: Surveillance, users and digital screen technologies. *International Journal of Cultural Studies, 13*(1), 5-24.

Blank, G. & Groselj, D. (2014). Dimensions of Internet use: amount, variety, and types. *Information, Communication & Society, 17*(4), 417-435.

Blank, G., & Lutz, C. (2018). Benefits and harms from Internet use: A differentiated analysis of Great Britain. New Media & Society, 20(2), 618–640.

boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday, 15*(8). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/3086/2589

Boyd, J. (2003). The rhetorical construction of trust online. *Communication Theory, 13*(4), 392-410.

Büchi, M., Just, N. & Latzer, M. (2017). Caring is not enough: the importance of Internet skills for online privacy protection, *Information, Communication & Society, 20*(8), 1261-1278.

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior, 81*, 42-51.

Clarke, R. (2014). Privacy and social-media an analytical framework. *Journal of Law, Information & Science, 23*(1), 1-23.

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). Online trust: Concepts, evolving themes, a model. *International Journal of Human-Computer Studies, 58*, 737-758.

Courtney, K. (2008). Privacy and senior willingness to adopt smart home information technology in residential care facilities. *Methods of Information in Medicine, 47*(1), 76-81.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83-108.

Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society*. https://doi.org/10.1177/2053951716679678

Dhir, A., Kaur, P., Lonka, K., & Nieminen, M. (2016). Why do adolescents untag photos on Facebook? *Computers in Human Behavior, 55*(B), 1106-1115.

Dinev, T., & Hart, P. (2006). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10*(2), 7-29.

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp 19-32). Heidelberg: Springer.

European Commission (2011). Special eurobarometer 359: *Attitudes on Data Protection and Electronic Identity in the European Union*. Retrieved from: http://ec.europa.eu/public_opinion/index_en.htm

European Commission (2015). *Special eurobarometer 431: Data protection*. Retrieved from: http://ec.europa.eu/public_opinion/index_en.htm

European Commission (2016). *Flash Eurobarometer 443: Report e-Privacy*. Retrieved from: https://doi.org/10.2765/209978

Flyverbom, M., Deibert, R., & Matten, D. (2017). The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business. Business & Society. https://doi.org/10.1177/0007650317727540

Flyverbom, M. (2017). Datafication, transparency and trust in the digital domain. In European Commission (Ed.), Trust at risk. Implications for EU policies and institutions (pp. 69-84). Luxembourg: Publications Office of the European Union. Retrieved from https://publications.europa.eu/es/publication-detail/-/publication/e512c11b-e922-11e6-ad7c-01aa75ed71a1

Gluck, J., Schaub, F., Friedman, A., Habib, H., Sadeh, N., Cranor, L. F., & Agarwal, Y. (2016, June). *How short is too short? Implications of length and framing on the effectiveness of privacy notices.* Paper presented at the Symposium on Usable Privacy and Security (SOUPS), Denver, CO.

Gürses, S. & Diaz, C. (2013). Two tales of privacy in online social networks. *IEEE Security & Privacy, 11*(3), 29-37

Hammersley, B. (27.03.2017). Concerned about Brexit? Why not become an e-resident of Estonia? *Wired*. Retrieved from http://www.wired.co.uk/article/estonia-e-resident

Hargittai, E. (2008). The digital reproduction of inequality. In D. Grusky (Ed.), *Social stratification* (pp. 936-944). Boulder, CO: Westview Press.

Hichang, C., Rivera-Sánchez, M., & Sun Sun, L. (2009). A multinational study on online privacy: global concerns and local responses. *New Media & Society, 11*(3), 395-416.

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (14.04.2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? Retrieved from: https://ssrn.com/abstract=1589864.

Hoy, M. G., & Milne, G. (2010) Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising, 10*(2), 28-45.

Hull, G. (2015). Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. *Ethics and Information Technology, 17*(2), 89-101.

Joinson, A. N., Houghton, D. J., Vasalou, A., & Marder, B. L. (2011). Digital crowding: Privacy, self-disclosure, and technology. In S. Trepte & L. Reinecke (Eds.), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (pp. 33-46). Berlin: Springer.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal, 25*(6), 607-635.

Kennedy, H., Poell, T., & Dijck, J. van. (2015). Data and agency. *Big Data & Society.* https://doi.org/10.1177/2053951715621569

Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(1), http://dx.doi.org/10.5817/CP2016-1-2

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision- making model in electronic commerce: The role of trust, perceived risk, and their antecedents. D*ecision Support Systems, 44*, 544-564.

Krasnova, H., & N. Veltri. (2010, January). *Privacy calculus on social networking sites: Explorative evidence from Germany and USA.* Paper presented at the Hawaii International Conference on System Sciences, Koloa, Kauai, Hawaii.

Litt, E. (2013). Understanding social network site users' privacy tool use. *Computers in Human Behavior, 29*(4), 1649-1656.

Livingstone, S., Ólafsson, K., & Staksrud, E. (2011). S*ocial networking, age and privacy.* London: EU Kids Online. Retrieved from http://eprints.lse.ac.uk/35849

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*. https://doi.org/10.1177/2053951714541861

Mai, J.-E. (2016). Big data privacy: The datafication of personal information. *The Information Society, 32*(3), 192-199.

Marwick, A. & Hargittai, E. (2018). Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society*, DOI: 10.1080/1369118X.2018.1450432

McCosker, A. (2017). Data literacies for the postdemographic social media self. *First Monday, 22*(10). DOI: http://dx.doi.org/10.5210/fm.v22i10.7307

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems, 23*(2), 103-125.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York: New York University Press.

Ostherr, K., Borodina, S., Bracken, R. C., Lotterman, C., Storer, E., & Williams, B. (2017). Trust and privacy in the context of user-generated health data. *Big Data & Society, 4*(1), DOI: https://doi.org/10.1177/2053951717704673

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215–236. https://doi.org/10.1177/0093650211418338

Pavlou, P.A. (2011). State of the information privacy literature: where are we now and where should we go? *MIS Quarterly, 35*(4), 977-988.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.

Pybus, J., Coté, M., & Blanke, T. (2015). Hacking the social life of Big Data. Big Data & Society. https://doi.org/10.1177/2053951715616649

Raynes-Goldie, K. (2010) Aliases, creeping and wall cleaning: understanding privacy in the age of Facebook. *First Monday, 15*(1).

Robinson, L. (2009). A taste for the necessary. *Information, Communication & Society, 12*, 488-507. DOI: 10.1080/13691180902857678

Roots, A., Lilleoja, L., & Beilmann, M. (2016). Võrguühiskond kui missioloogiline võimalus: Kirjeldav osa. [*Network society as missiolocigal opportunity] In E. Jõks (Ed.). Kuhu lähed, Maarjamaa? — Quo vadis, Terra Mariana? [Where are you going, Maarjamaa - Quo vadis, Terra Mariana?*] (pp. 321-336). Tallinn: Eesti Kirikute Nõukogu.

Smith, A. (4.12.2014). Half of online Americans don't know what a privacy policy is. Factanck: News in Numbers. Retrieved from http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/

Smith, J., Hewitt, B., & Skrbis, Z. (2015). Digital socialization: Young people's changing value orientations towards internet use between adolescence and early adulthood. Information. *Communication & Society, 18*(9), 1022-1038.

Song, Z., Hao, C., & Daqing, Z. (2013). Empirical study on users' participation behavior in SNS based on theory of perceived risks and involvement degree. In Proceedings of the 2013 *10th International Conference on Service Systems and Service Management (ICSSSM) IEEE* (pp. 424-429). Hong Kong, China.

Taddicken, M. (2013). The "Privacy Paradox" in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance of different forms of self-disclosure. *Journal of Computer-Mediated Communication, 19*(2), 248-273.

Talebi, N., Hallam, C., & Zanella, G. (2017). The new wave of privacy concerns in the wearable devices era. In Proceedings of the *PICMET 2016 - Portland International Conference on Management of Engineering and Technology: Technology Management for Social Innovation* (pp. 3208-3214). Honolulu, Hawaii, USA. https://doi.org/10.1109/PICMET.2016.7806826

TRUSTe (2014). *TRUSTe privacy index*. Retrieved from https://www.trustarc.com/resources/privacy-research/

Tufekci, Z (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28*(1), 20-36

Turow J., Hennessy, M., & Draper, N. (2015). *The trade-off fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation*. Retrived from https://www.asc.upenn.edu/ sites/default/files/TradeoffFallacy_1.pdf

den Broeck, E. V., Poels, K., & Walrave, M. (2015). Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood. *Social Media + Society*. https://doi.org/10.1177/2056305115616149

Vihalemm, P., & Masso, A. (2017). 'Mina. Maailm. Meedia' metoodikast *[About the method of survey 'Me, the Media, and the World']. In P. Vihalemm, M. Lauristin, V. Kalmus, & T. Vihalemm (Eds.), Eesti ühiskond kiirenevas ajas: elaviku muutumine Eestis 2002-2014 Mina. Maailm. Meedia tulemuste põhjal [Estonian society in the acceleration of time: changes of lifeword in Estonia in 2002-2014]* (pp. 96-109). Tartu: University of Tartu Press.

Wakefield, R. (2013). The influence of user affect in online information disclosure. *Journal of Strategic Information Systems, 22*(2), 157-174.

Walrave, M., Vanwesenbeeck, I., & Heirman, W. (2012). Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 6*(1), http://dx.doi.org/10.5817/CP2012-1-3

Warner, M. R. (2013). *Applied statistics: from bivariate through multivariate techniques* (2nd ed.). Thousand Oaks, Calif: SAGE Publications.

Wright, D. (2017). Privacy and trust at risk in surveillance societies. In European Commission (Ed.), *Trust at risk. Implications for EU policies and institutions* (pp. 48-68). Luxembourg: Publications Office of the European Union. Retrieved from https://publications.europa.eu/es/publication-detail/-/publication/e512c11b-e922-11e6-ad7c-01aa75ed71a1

Xu, H., Dinev, T., Smith H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: toward an integrative view. In proceedings of *International conference on information systems (ICIS) ICIS 2008*. Paris, France. Retrived from http://faculty.ist.psu.edu/xu/papers/conference/icis08a.pdf.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 798-824.

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society, 16*(4), 479-500

**Maris Männiste** is a media and communication doctoral student and information systems assistant at the Institute of Social Studies of the University of Tartu. Her research interests include people's perceptions of privacy, datafication practices and peoples' attitudes and everyday practices related to personal informatics systems (e.g. self-tracking, self-monitoring but also monitoring children).

**Anu Masso** is a senior researcher at the Institute of Social Studies of the University of Tartu, and a visiting researcher at ETH Zürich. Her research interests include various forms of social transformations related to spatial mobility, e.g. everyday activity spaces, immigration attitudes, and media mobility. Her special passion is research methods, e.g. methodological shifts related to digital technologies and critical data studies.

## Acknowledgement

The preparation of this paper was supported by a grant from the Estonian Ministry of Education and Research (IUT 20-38).

## Appendix

**Table 2:** Descriptive statistics of privacy concerns

| | N | Mean | Std. Deviation |
|---|---|---|---|
| Foreigners | 780 | 1.81 | 1.06 |
| Governmental institutions (police, tax board, etc.) | 778 | 1.70 | 1.11 |
| Business institutions | 780 | 1.69 | 1.11 |
| Friends and acquaintances | 779 | 1.60 | 0.94 |
| Local governmental institutions | 779 | 1.51 | 0.96 |
| Employer | 780 | 1.46 | 0.92 |
| Family members | 779 | 1.39 | 0.83 |
| Health system | 780 | 1.38 | 0.79 |
| Educational system | 780 | 1.38 | 0.79 |

*Source:* authors' calculations, based on data from the survey "Me. The World. The Media".

**Table 3:** Regression analysis of the concerns about privacy (GLM)

| | | Model 1: Concerns regarding institutional privacy | | Model 2: Concerns regarding individual privacy | | Model 3: Concerns regarding privacy (total) | |
|---|---|---|---|---|---|---|---|
| | | B | SE | B | SE | B | SE |
| Socio-demographic variables | Intercept | -.187*** | .044 | -.218*** | .045 | -.281*** | .043 |
| | Age | .040 | .044 | -.137** | .045 | -.052 | .042 |
| | Gender | -.086* | .035 | .004 | .036 | -.065* | .034 |
| | Language | -.066 | .037 | -.004 | .038 | -.054 | .036 |
| | Education | .072* | .037 | -.034 | .038 | .037 | .036 |
| | Income | -.046 | .034 | -.001 | .034 | -.037 | .033 |
| | Perceived social status | -.057 | .040 | .028 | .041 | -.028 | .039 |
| Variables measuring social media use and habits | Self-expression and communication-centred Internet use | .128** | .050 | .007 | .051 | .106* | .048 |
| | Use of various social media channels | .055 | .048 | .076 | .048 | .090* | .046 |
| | Concerns about mobile or smartphone overuse in the vicinity | .118*** | .035 | .182*** | .036 | .204*** | .034 |
| | Functional versatility of social media use | .087* | .041 | .073 | .041 | .114** | .039 |
| | Enterprisingness | .124*** | .035 | .062 | .035 | .136*** | .034 |
| Variables measuring trust in institutions | Trust in representatives of governmental institutions | -.125*** | .036 | -.001 | .036 | -.100** | .034 |
| | Trust in other state institutions | -.066* | .034 | .009 | .035 | -.047 | .033 |
| | Trust in media institutions | -.075* | .039 | -.033 | .039 | -.079* | .037 |
| | Trust in cultural / surveillance institutions | -.046 | .035 | .011 | .036 | -.030 | .034 |
| | *AIC* | *2098.208* | | *2121.333* | | *2040.890* | |
| | *Likelihood Ratio Chi-square* | *101.899**** | | *87.967**** | | *153.672**** | |

*Note:* *p<.05; **p<.01; ***p<.001
*Source:* authors' calculations, based on data from the survey "Me. The World. The Media".