The Researching and Teaching Communication Series

Journalism, Representation and the Public Sphere

edition lumière
Bremen 2015

Bibliographische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über http://dnb.ddb.de abrufbar.

ISBN: 978-3-943245-37-0

JOURNALISM, REPRESENTATION AND THE PUBLIC SPHERE

Edited by: Leif Kramp, Nico Carpentier, Andreas Hepp, Ilija Tomanić Trivundža, Hannu Nieminen, Risto Kunelius, Tobias Olsson, Ebba Sundin and Richard Kilborn.
Series: The Researching and Teaching Communication Series
Series editors: Nico Carpentier and Pille Pruulmann-Vengerfeldt
Photographs: François Heinderyckx (section photographs)
Print run: 600 copies
Electronic version accessible at: http://www.researchingcommunication.eu and http://www.comsummerschool.org

The publishing of this book was supported by the University of Bremen, the European Communication Research and Education Association (ECREA) and the Slovene Communication Association.

The 2014 European Media and Communication Doctoral Summer School (Bremen, August 3-16) was sponsored by the German Academic Exchange Service (DAAD) and significantly funded at the expenses of the Federal Foreign Office (AA). It was also supported by the University of Bremen, ZeMKI, Centre for Media, Communication and Information Research, the „Communicative Figurations“ research network, the Graduate Center of the University of Bremen (ProUB) and by a consortium of 22 universities. Affiliated partners of the Summer School were the European Communication Research and Education Association (ECREA) and the International League of Higher Education in Media and Communication (MLeague).

Table of Contents

SECTION 3: Public Sphere, Space and Politics

SECTION 4: Rethinking Media Studies

SECTION 5: Academic Practice

PART 2
The European Media and Communication Doctoral Summer School 2014 and its Participants

“I have nothing to hide”. A coping strategy in a risk society

Maria Murumaa-Mengel, Katrin Laas-Mikko & Pille Pruulmann-Vengerfeldt

Abstract

The right to control and limit access to one’s information is increasingly discussed not only in the context of governments, but also within big multi-national companies. Estonia is proud of its emerging e-state, where increasing number of services are being provided online with more and more data collected about citizens. The Soviet past of living under the watchful eye of “Big Brother” makes Estonia an interesting and unique case for studying informational privacy. Many have argued that in the modern society, if you have done nothing wrong, then you have nothing to hide, using this argument as a way to legitimize loss of privacy. This article explores how the “nothing to hide” -argument can be conceptualized as a coping strategy in complex informational privacy situations. We will introduce some of the results of a nationally representative Estonian survey, “Right to privacy as a human right and everyday technologies”, aimed at studying people’s general understanding of privacy and perception about various potentially privacy invasive situations. Whether acknowledged or not, people are in a state of constant stress – they think many of the actors (the state, employers, enterprises and other people) could jeopardize their privacy, and yet at the same time, they are routinely in situations where their information is collected. To cope with the privacy invasive situations and practices, many have adopted the belief that they have nothing to hide. This strategy, while functional for the individual, means that structurally people adopt self-censorship strategies or slowly lose trust in the society at large.

Keywords: informational privacy, coping strategies, survey data on privacy, Estonia

---

Murumaa-Mengel, M., Laas-Mikko, K., Pruulmann-Vengerfeldt, P. (2015) ‘“I have nothing to hide”. A coping strategy in a risk society’, pp. 195-207 in L. Kramp/N. Carpentier/A. Hepp/I. Tomanić Trivundža/H. Nieminen/R. Kunelius/T. Olsson/E. Sundin/R. Kilborn (eds.) *Journalism, Representation and the Public Sphere*. Bremen: edition lumière.

1. Introduction

The concept of privacy can include a wide variety of interests, rights and aspects. Daniel Solove (2002) names six aspects of privacy: the right to be left alone; restricted access to one's person (physical person), or the possibility to protect oneself from unauthorised access; the right to hide certain things from others; control over personal information; protection of one's dignity, individuality and persona; and intimacy – the right to control and limit access to information that concerns intimate relationships and aspects of life. In this study, the right to hide information is chosen as the main focal point.

Although the literature on privacy stresses the subjectivity and context-sensitivity, there have been several attempts using questionnaires to examine privacy-related perceptions (e.g. European Commission, 2011). Our study focuses on perceived threats to privacy and people's general beliefs and attitudes towards the access, collection and use of their data.

In order to open the discussion around the "nothing to hide" argument in Estonia, we rely on data collected from face-to-face personal surveys using a standardised questionnaire carried out from May to June 2014. The representative sample (n=1000) consists of permanent residents of the Republic of Estonia aged 15-74. Interviews were conducted in the respondents' homes in either Estonian or Russian, as roughly 25% of the Estonian population is Russian (Population by sex, ethnic nationality and county, 2014). For proportional representation respondents were chosen randomly and separate weighting was carried out in accordance with the theoretical model of the target group. The final number of respondents was 959. The results of the survey can be extended to the whole Estonian population of the appropriate age, as the margin of error did not exceed 3.09 per cent.

Estonia is a particularly interesting country to analyse privacy-related discussions. On the one hand, the country's population is very enthusiastic about new technologies, accepting new inventions very easily. On the other hand, past experience with the Soviet regime should have made Estonians wary and apprehensive about any kind of surveillance. In his discussion at the Estonian Institute of Human Rights conference Prof. Simon Davies pointed out this conundrum and was baffled about the lack of concern among the Estonian population about privacy (Video Recordings of the Conference, I Panel, 2014). The following article briefly shares some of the results from the aforementioned survey to problematize the "nothing to hide" paradox in a post-Soviet context. In order to do that, we will briefly give an overview of the Estonian context and the theoretical discussion surrounding the "nothing to hide" argument. We then introduce the Estonian data and conclude that in order to cope with privacy risks and confusing practices, many respondents have indeed adopted the belief that they have nothing to hide.

2. Estonia – from Soviet to Skype

Estonia's history as a member of the Soviet Union is a prime example of mutual surveillance and collective correction (Zdravomyslova and Voronkov, 2002), although as a border-area, both Western and Soviet conceptions and patterns were always present and combined in Estonian everyday practice (Kannike, 2006). In the Soviet Union, people were mostly unable to execute their right to privacy, as both working life and family life were subjected to state observation and control (Zdravomyslova and Voronkov, 2002). Furthermore, Kannike (2006: 216) claims that while in "*Western civilization privacy is intimately connected with the notion of home, the concept of privacy has never been a feature of Russian or Soviet culture*". It could be argued that during the Soviet period Estonians did not have much control over their information, so instead they valued privacy in physical space – their homes (Kurg, 2004). In addition, people in different over-controlling regimes have throughout history developed coping mechanisms and strategies to maintain their privacy, at least to a certain extent (boyd, 2008).

Presently, Estonia has earned positive recognition in the world for its diverse and widely used national e-solutions (electronic identity card, electronic tax returns, e-voting, paperless government, e-health, e-commercial register, e-school, education information system, etc.). Over 80% of Estonians use the internet regularly (Information technology in household, 2014) and find that online services have had a clearly positive impact on their lives by helping them save time and making paperwork easier to handle (Kalvet, Tiits and Hinsberg, 2013). These two factors – perceived usefulness (with a focus on the objective) and perceived ease-of-use (with a focus on the process) have a central position in the technology acceptance model (Davis, 1989). A couple of years ago, every second Estonian had used the state portal eesti.ee (Citizens' satisfaction with with state's public e-services, 2012), which combines state and municipal e-services, information on various areas of life and the contact data of public authorities. The state portal eesti.ee also enables the cross-usage of data between different registers and databases based on the identity code of the person and the technical data exchange layer called X-road. In our experience, this is a practice Estonians are proud of, but would not be possible in many other countries which, contrary to Estonians, see the link between the identity code, which is a unique personal identifier, and cross-usage as a very problematic mass surveillance-enabling practice (See also discussions in Germany Hornung and Schnabel, 2009). As new registries and databases are created and the old ones are updated, modern (democratic) states need to pay attention to different aspects of citizens' privacy.

Although data is nowadays collected, processed and stored in many databases and cross-used, most people pay little attention to this, or they find it unimportant – only 40% of Estonians agreed with the 2011 Eurobarometer claim that the government is asking for more and more personal information, whereas the European average was much higher – 64% (European Commission, 2011). In Estonia, the reason people don't consider it to be that relevant a question with regards to their privacy may be due to the policy decision that wherever possible, data is reused from existing databases, and new data is only collected on a need-to-know basis. Also, people are able to retrieve information about who has used/seen their data from the same eesti.ee online portal or in related databases.

3. The "Nothing to Hide" fallacy

The nothing to hide argument is frequently used in public discussions about the legitimacy of surveillance practices. It appears in different forms. This argument usually justifies the mass surveillance by bearing down on the conscience of people, where the example claim could be: "if you have nothing to hide, then you have nothing to fear" (for other different forms of argument see Solove, 2007). While originally nothing to hide arguments referred to the surveillance practice of governments, since arguably only governments have limitless resources to conduct mass surveillance, today this appears to be not true. Google, Amazon and Facebook, U.S. tech giants certainly have the motivation and resources. In order to discuss what is wrong with the argument "I have nothing to hide" we need to open up the concept of privacy.

The concept of privacy can include a wide variety of interests, rights and aspects. We focus primarily on informational privacy, which concerns the data collected, recorded and shared about a person. Several privacy theoreticians (Westin, 1967; Rachels, 1975) consider the central notion of privacy to be control over personal information. Westin (1967) defined privacy as the right of individuals, groups or institutions to decide when, how and to what extent the information related to them is communicated to others. This means that the extent of privacy or the feeling of whether privacy has been violated or not depends on the data subject's choice as to how well and what kind of information he or she wants protected. This is based on the liberal idea of self-determination – a person determines his or her self and decides freely the values that he or she holds dear. The idea of control seems all-encompassing and absolute, which is why the modern concepts of privacy tend to narrow the scope of the term, and emphasize a person's right to decide who and to what extent someone can access and use information concerning him or her (Rössler, 2005; Moore, 2008). In this respect, the right to privacy includes control over access

as well as over information usage rights. At the core of this right is the person's (informed) consent to have his or her personal data collected/accessed for a specific purpose, such as the purchase of something from an online store. This consent does not automatically mean that the data can be used in some other context or circumstances for some other purpose, as often is the case of surveillance.

Discussions over privacy that take place in the public and academic spheres reflect the risk discourse – privacy is perceived as a constantly endangered value, which undoubtedly needs protection. Therefore, it is important to discuss what we protect while protecting privacy and what is at risk when we don't.

Some scholars, such as Simson Garfinkel (2001) and David Brin (1998), have claimed that privacy is dead and that we should get used to the thought that our society is extremely transparent. Mark Zuckerberg, the founder of Facebook, has said (Kirkpatrick, 2010) that the era of privacy is over and that only those people who have something to hide worry about the lack thereof. The inherent logical error of this argument has been pointed out by Solove (2007), who says that the claim is based on the false presumption that privacy means hiding bad deeds and wrong behaviour. The people who play the I-have-nothing-to-hide card often mean that they do not have anything to hide from a *particular* audience whom they imagine while sharing information. They do not mean that they have nothing to hide from absolutely anyone who could potentially reach that information, especially in online settings (Siibak and Murumaa, 2011).

According to Valeria Steeves (2009), privacy helps us create meaningful relationships with others. She argues that striving for privacy is a social practice which allows social actors to draw a line between themselves and others, thereby, being open or closed to social communication. In accordance with this theory, social actors are capable of choosing what is most important for them and defining themselves in relationships. The protection of personal autonomy and the right to define him- or herself in social context is the reason why we should not give over our privacy.

Value conflicts and choices between different values are seen today as a natural part of the pluralist society and privacy should be weighed against other important and sometimes incomparable values (Steeves, 2009; Nissenbaum, 2010). We risk daily the invasion of our privacy by publishing sensitive information about ourselves in significant relationships or social environments; generally, we do not want "perfect privacy" – that is, complete separation, anonymity or exclusion from social relations. Therefore, as mentioned earlier – context matters.

When comparing value of privacy against value of security, privacy is often characterized as an individual and security as a societal value or interest; in a value conflict, the societal interest will be preferred. (Himma, 2007; Solove, 2007). Violation of the right to privacy can result in many undesirable consequences for a person, such as identity theft and access to person's property or benefits; injustice caused by misuse of certain information; unequal treatment or harm to one's dignity. Some scholars (Gavison, 1980; Steeves, 2009) claim that privacy also has societal importance; it is essential to democratic government or social relations since it fosters the moral autonomy of persons, who are central to those concepts. However, privacy violation risks to society are difficult to assess because as a rule we are dealing with so-called soft impacts and impacts in degree (not totally). We cannot say exactly how many people need to feel that their privacy has been invaded and in which context it needs to happen so that people would lose trust in government institutions or that democracy would be endangered.

The asymmetrical information and lack of transparency of surveillance practices and how the data are analyzed puts citizens in a disadvantaged position. The surveillance practices do not violate only the right of privacy, but personal autonomy. As noted by Solove (2007), this is a structural problem. The question here is not that all surveillance practices are inherently unjustified. Rather, there is a need to discuss these issues in public, declare and enact clear principles about justified surveillance practices and technologies; maintain independent and democratic control mechanism to get oversight how these rules are followed.

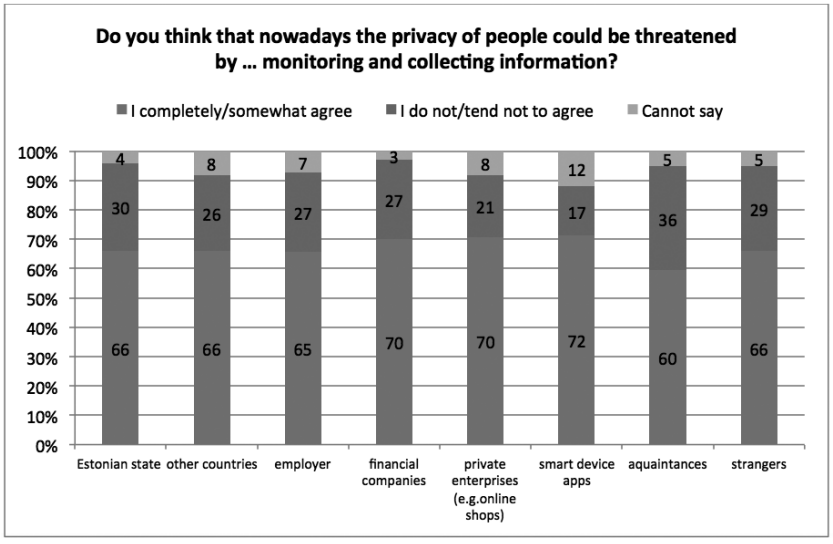
In our empirical sections we first explore, through data, which actors are perceived as a threat to people's informational privacy. Then, we look at the attitudes people express about collection, access and use of their information in general.

4. Everything is a threat to privacy...

To establish if the discussions about privacy are only relevant in the academia and the policy domains, we asked our respondents to which extent they agreed or disagreed with the statement "The worry about the safety of personal data is exaggerated". The majority of respondents (53%) were of the opinion that being worried about personal data is relevant, however, the share of people who find that the whole issue has been exaggerated is also significant – 41%. This shows that while many people are concerned about the issue, many have adopted an attitude of not caring as one of their coping mechanisms in this confusing situation.

In order to understand who and what is perceived as a potential threat, we asked the respondents to rate different actors on the basis of whether those would be considered to be threatening to people's privacy (Figure 1). A majority of respondents find all the listed actors to be potential risks (60-72% agreement rate regarding different actors).

Figure 1: To what extent are different parties perceived as threats to privacy (% of respondents, n=959)



People find the biggest threat to their privacy to be information collection via smart devices (mobile phones, tablets) and applications, but there were also many who answered "I don't know" (12%) because they simply had not come into contact with these technologies. Acquaintances were seen as the least threatening in relation to the monitoring and collecting of information.

"*Everything is a threat*" or that "*we live in the risk society*" (Beck, 1992) perception is undoubtedly partly rooted in the media frames related to the topic – subject matter included in public discussions is adopted into personal risk perceptions. In the aftermath of 9/11, a "securitization" discourse also emerged in which security issues are dealt with at an accelerated rate and therefore may be allowed to violate normal social rules (Hansen and Nissenbaum, 2009). This has enforced the view that national or collective security is by default more important than other rights and values, especially privacy. In recent years, the

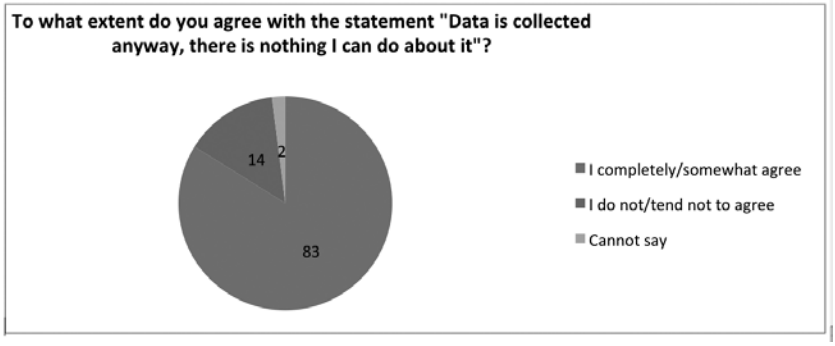
media have covered many cases of information misuse by tech giants (Google, Facebook, etc.) and governments, which have raised awareness of the topic among citizens.

Returning to Figure 1, we see that 66% of respondents think that the Estonian state could be a threat to people's privacy. Curiously, when in another question we divided "the state" into more specific actors (medical and educational institutions, local government) and posed the question in the form of "*how do you feel your data is being used*", contradictory evidence emerges: the level of trust was 89-71%. We can notice contradictions and confusion in people's answers, as it is often a topic that is hard to grasp. People seem to perceive risks to privacy and the topic as relevant, so one might presume that they should see their role as active.

5. ...but there is nothing I can do about it!

A sort of fatalist attitude, an accepting of the unpleasant state of things, which became evident in the Eurobarometer privacy survey (European Commission, 2011), can be seen in our study as well. 83% of the respondents agreed with the statement about data being collected anyway and a person ultimately having no control over it (Figure 2).

Figure 2: To what extent do people agree to the claim about data being collected despite their preferences (% of all respondents, n=959)



In addition, as pointed out in the previous section, a large proportion of people think that it is important to be worried about the protection of personal data, but 74% of respondents also agreed with the claim "I have nothing to hide". To a limited extent, we see that this is more common in the case of older people (70% among 25-34-year-olds, 79% among 65-74-year-olds). Considering Estonia's totalitarian regime history and people's experiences and past everyday practices that many still remember, this could be interpreted as a distancing coping mechanism. Folkman and Lazarus (1988) said that such avoidance, among other emotion-focused coping strategies, that was oriented toward managing the emotions of stress and everyday life in USSR was a source of deep cultural stress (Kannike, 2006). On the other hand, as Kannike (2006: 225) points out, during many Soviet years, "*the main slogan was opening up the private sphere to the state and the collective*", and this message might still be embedded in collective consciousness, which is why we see a higher percentage of agreement in older age groups. This finding is rather paradoxical, as Soviet history has also left people with the practices of counterculture, hidden meanings, double thinking and practices (one for the public self, one for the private self) (Kreegipuu, 2011).

There are a couple of possible explanations behind previously mentioned contradictions in our results - everything is perceived as a potential threat, but at the same time people express trust in particular institutions and feel they have nothing to hide. From a utilitarian perspective the perceived trade-off can simply be appealing enough and this makes it easier to hand out information about oneself and friends. The most common motivator for a trade-off is tied to the consumption of a product or service – to use a web environment one needs to disclose personal data. A step further – in order to use the service or product even more easily or efficiently, one needs to provide more information, and so on. The Eurobarometer study on privacy (European Commission, 2011) shows that the most significant reason as to why people disclose personal information is to use a service in either a social network or e-commerce (61% and 79% respectively). Similarities occur in other domains as well (e.g. communication with the state is less complicated via e-channels, it is easier to find one's data in one cross-database, etc.).

Additionally, Estonians stand out in cross-country comparisons because of significantly higher government trust rates – in 2014 trust in the government was 44% in Estonia, the EU average was 26% (European Commission, 2014). One possible explanation can be that the positive discussion around Estonia's e-state and the advances around it make critical discussions and considerations almost invisible even in the mainstream public debate/sphere. The years of living under foreign rule may have meant that "Estonia's own state" is regarded with trust and sense of ownership that allows less uncritical attitudes.

6. Conclusion

We should ask ourselves why we as a society should not tolerate the claim, "I have nothing to hide". In reality, everyone has something to hide from others (Solove, 2007). We are not only talking about covering up socially unacceptable or embarrassing behaviour, thoughts and convictions by sheltering behind the shield of the right to privacy. Privacy is primarily valued because it protects people's freedom of choice to disclose personal information as they see fit.

Nowadays, personal responsibility is often stressed and the public has accepted the discourse - people frequently think that the responsibility for personal data on the Internet falls on the individual (European Commission, 2011). For regulators and legislators, it is easy to see the individual as responsible (for digital literacy as well as privacy) and people have adopted this point of view. Privacy decisions are based on complex, subjective perceptions of threats and potential damage, psychological needs, and actual personal returns play an important role and affect our decisions (Acquisti and Grossklags, 2007). But the problem is that we usually lack complete information about technologies which themselves are very often technically complex and non-transparent regarding data processing practices and possible consequences. Once again, such a complex situation can trigger mental disengagement from the subject, and acceptance of the "I have nothing to hide" argument.

If the state or large corporations ignore the right to privacy, it primarily violates an individual's freedom of choice and decreases general trust in these institutions (and in the state in general regarding state authorities). Such practices could encourage the spread of the self-censoring strategy. Several researchers have stated that the strategies that are based on minimum content creation and users' low activity level can have a negative impact on maintaining and developing friendships (Marwick, Murgia-Diaz and Palfrey, 2010; Larsen, 2007).

Whether acknowledged or not, people in Estonia and in many other countries saturated with modern technologies are in a state of constant stress – they believe their privacy is threatened by various parties but have to cope with an everyday life context in which their information is constantly accessed, collected and used. We have argued in this text, that "nothing to hide", while routinely used as coping strategy, is not an acceptable solution. Instead, the state and big corporations need to take steps to support the individual by making their information use more transparent and helping people to understand more clearly whether and to which extent they need to fear about information being disclosed. In the society where we live, these responsibilities need to be shared in order to be adequately managed.

Acknowledgements

The authors are grateful for the support of Estonian Science Fund personal grant PUT44 and Estonian Institute of Human Rights for funding the survey.

References

Acquisti, A., Grossklags, J. (2007) 'What can behavioural economics teach us about privacy?', pp. 363-377 in A. Acquisti, S. Gritzalis, S. Di Vimercati and C. Lambrinoudakis (Eds.) *Digital Privacy: Theory, Technologies, and Practices*. Auerbach Publications.

Beck, U. (1992) *Risk Society: Towards a New Modernity*. New Delhi: Sage.

Boyd, D. M. (2008) *Taken Out of Context: American Teen Sociality in Networked Publics*. Dissertation. University of California, Berkeley. Downloaded on 11 January 2015 from http://www.danah.org/papers/TakenOutOfContext.pdf

Brin, D. (1998) *The Transparent Society.* Reading, MA: Perseus Books.

Davis, F. D. (1989) 'Perceived usefulness, perceived ease of use, and user acceptance of information technology', *MIS Quarterly*, 13(3): 319-340.

Folkman, S., Lazarus, R. S. (1988) 'Coping as a mediator of emotion', *Journal of Personality and Social Psychology*, 54(3): 466-475.

Garfinkel, S. (2001) *Web Security, Privacy and Commerce*. Sebastopol, CA: O'Reilly.

Gavison, R. (1980) 'Privacy and the limits of law', *The Yale Law Journal*, 89(3): 421-471.

Hansen, L., Nissenbaum, H. (2009) 'Digital disaster, cyber security, and the Copenhagen school', *International Studies Quarterly*, 53: 1155-1175.

Himma, K. E. (2007) 'Privacy versus security', *San Diego* Law Review, 44: 859-919.

Hornung, G., Schnabel, C. (2009) 'Data protection in Germany I: The population census decision and the right to informational self-determination', *Computer Law & Security Review*, 25(1): 84-88.

Kalvet, T., Tiits, M., Hinsberg, H. (2013) *The Impact and Effectiveness of E-Services [E-teenuste kasutamise tulemuslikkus ja mõju]*. Tallinn: Institute of Baltic Studies and Poliitikauuringute Keskus Praxis.

Kannike, A. (2006) 'Creating cultural continuity in the domestic realm: the case of Soviet Estonia', *Acta Historica Tallinnensia*, 10: 212-229.

Kirkpatrick, M. (2010) 'Facebook's Zuckerberg says the age of privacy is over', *Readwrite*. Downloaded on 11 January 2015 from http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php

Kreegipuu, T. (2011) *The Ambivalent Role of Estonian Press in Implementation of the Soviet Totalitarian Project.* Dissertation. Tartu University. Tartu: Tartu University Press.

Kurg, A. (2004) 'Almanac: art and home 1973-1980 [Almanahh Kunst ja Kodu 1973-1980]', *Studies on Art and Architecture*, 2(13): 110-142.

Larsen, M. C. (2007) '35 Perspectives on online social networking', *Social Computing Magazine*. Downloaded on 11 January 2015 from http://vbn.aau.dk/files/17515817/35_Perspectives_on_Online_Social_Networking_by_Malene_Charlotte_Larsen.pdf

Marwick, A. E., Murgia-Diaz, D., Palfrey, J. G. (2010) 'Youth, privacy and reputation (literature review)', *Berkman Center Research Publication*, 2010(5); Harvard Public Law Working Paper No. 10(29), http://dmlcentral.net/sites/dmlcentral/files/resource_files/YouthPrivacyReputationBERKMAN.pdf

Moore, A. (2008) 'Defining privacy', *Journal of Social Philosophy*, 39: 411-428.

Nissenbaum, H. (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press.

Rachels, J. (1975) 'Why privacy is important?', *Philosophy and Public Affairs*, 4: 323–333.
Rössler, B. (2005) *The Value of Privacy*. Polity Press.
Siibak, A., Murumaa, M. (2011) 'Exploring the 'nothing to hide' paradox: Estonian teens' experiences and perceptions about privacy online', *Conference article, A Decade In Internet Time: OII Symposium on the Dynamics of the Internet and Society*, Oxford, 21-24 September. Downloaded on 11 January 2015 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1928498
Solove, D. J. (2002) 'Conceptualizing privacy', *California Law Review,* 90: 1087-1155.
Solove, D. J. (2007) '"I've got nothing to hide" and other misunderstandings of privacy', *San Diego Law Review*, 44: 746-771.
Steeves, V. (2009) 'Reclaiming the social value of privacy', pp. 191-208 in I. Kerr, V. Steeves, and C. Lucock (Eds.) *Privacy, Identity and Anonymity in a Network World: Lessons from the Identity Trail*. New York: Oxford University Press.
Zdravomyslova, E., Voronkov, V. (2002) 'The informal public in Soviet society: double morality at work', *Social Research*, 69(1): 49-69.
Westin, A. (1967) *Privacy and Freedom*. New York: Atheneum.
Ministry of Economic Affairs and Communications (2012) 'Citizens' satisfaction with state's public e-services'. Downloaded on 11 January 2015 from https://www.mkm.ee/sites/default/files/content-editors/failid/E_riik/uuring_kodanike_rahulolu_riigi_poolt_pakutavate_avalike_e-teenustega_2012_emor.pdf
'Information technology in household'. (2014) Statistics Estonia. Downloaded on 11 January 2015 from http://www.stat.ee/database
Statistics Estonia (2014) 'Population by sex, ethnic nationality and county'. Downloaded on 11 January 2015 from http://www.stat.ee/database
European Commission (2011) 'Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union'. Downloaded on 11 January 2015 from http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
European Commission (2014) 'Special Eurobarometer 415: Europeans in 2014'. Downloaded on 11 January 2015 from http://ec.europa.eu/public_opinion/archives/ebs/ebs_415_data_en.pdf
Video recordings of the Conference, I Panel. (2014) Estonian Institute of Human Rights. Downloaded on 11 January 2015 from http://www.eihr.ee/en/annualconference/annual-conference-2014/live2014/

Biographies

Maria Murumaa-Mengel is a Junior Research Fellow of Media Studies and a PhD student at the Institute of Social Sciences of the University of Tartu. Her PhD thesis is about the transformation of the meaning of privacy and imagined audiences in social media. Maria is currently involved in research projects focusing mainly on media education and inter-generational relationships in the information society.

Contact: maria.murumaa@ut.ee

Katrin Laas-Mikko works at the Estonian Certification Centre as a quality manager, and is doing her doctorate at Tartu University. Her thesis is connected to moral aspects in the context of new technologies and the risks associated with them. She has participated in several projects of The European Union that have been related to technologies of identity and privacy (RISE, TECHNO-LIFE, FIDELITY, etc.) through the Centre of Ethics at the University of Tartu and The Institute of Baltic Studies.

Contact: katrin.laas-mikko@ut.ee

Pille Pruulmann-Vengerfeldt is professor of media studies in the University of Tartu, Institute of Social Sciences and a researcher in Estonian National Museum. Her interests are internet user typologies, user-friendly online spaces as possible venues for participation and participatory applications for organisations. She is leading and participating in several national and international projects. Her recent publications include among other things collection Democratising the Museum: Reflections on Participatory Technologies (2014) Peter Lang Verlag edited together with Pille Runnel.

Contact: pille.vengerfeldt@ut.ee