THE RIGHT TO PRIVACY AS A HUMAN RIGHT AND EVERYDAY TECHNOLOGIES

Methodology and results of the study

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

TABLE OF CONTENTS

METHOD AND SAMPLE

The "Right to privacy as a human right and everyday technologies" was a pan-Estonian poll commissioned to collect empirical material for the study. Although the preceding literature overview stresses the subjectivity and context-sensitivity of privacy, there have been several attempts to examine privacy-related perceptions with questionnaires. We had to limit ourselves to a reasonable number of questions and, as a result, we were forced to make several difficult choices and leave out many important topics; therefore, our questionnaire was not as detailed and context-sensitive as we would have liked it to have been. The questions were asked as part of an omnibus study and, therefore, the relevant questionnaire was filled out in between other topics, which might have had some impact on responses. The whole questionnaire has been included in Annex 1.

Despite the fact that when compiling the questionnaire we tried to take as neutral and diverse an approach to privacy as possible, the general tone of the questions tends to be that people perceive new information and communication technologies as privacy-invading and threatening. Therefore, the questionnaire does not include a question as to whether new technologies provide more opportunities for privacy, but instead we have asked to which extent new technologies are viewed as dangerous and privacy-invading. This postulation might prejudice the respondents to be more critical in the assessment of dangers and problems but, as possible responses include neutral answers and answers that refer to the exaggeration of the issue, we hope that the respondents have not been directed more than is absolutely necessary.

We would like to stress once more that the study focuses on perceived threats to privacy, not objective violations of privacy, and that our task was not to determine whether a specific situation constitutes a violation of privacy or not. Since it is difficult to draw clear-cut lines in relation to privacy, we were more interested in how people interpret the whole topic of privacy in their mind.

SAMPLE AND QUESTIONING

The sample was selected and actual questioning was conducted by Turu-Uuringute AS, which provided the description of the technical side of the study. The sample of the study consists of permanent residents of the Republic of Estonia aged 15 and older; the analysis included respondents from the age of 15 to 74. The size of the sample was 1,000 people.

Respondents were chosen randomly, so that all Estonian counties and settlement types would be represented proportionally. The territorial model of the sample was compiled on the basis of the population statistics database of the Statistical Office. In the first stage of random selection, 100 points were found across Estonia and, in the second stage, specific interviewees were chosen in these points. The locations of points by counties and settlement types were determined based on actual population distribution. Using 100 points in population surveys ensures sufficient coverage on the territory of Estonia.

In address selection, the source address method was applied, in which case each interviewer is given a randomly chosen address for the first interview. From there, interviewer moves on at a certain interval – visiting each third apartment or second private house – to ensure the randomness of the selected dwellings.

In respondent selection, the so-called youngest male rule was applied, which means that the interview is requested from the youngest male at home who is at least 15 years old. If there are no men at home, the youngest applicable female is preferred.

The method of questioning was a face-to-face personal interview with a standardised questionnaire. Interviews were conducted in the respondents' homes in either Estonian or Russian. Questions were asked by 60 specially trained interviewers from Turu-uuringute AS. The survey was carried out from 27th of May to 15th of June 2014 (Table 1).

To check the questioning process, 100 letters were sent out to determine whether the questioners actually visited the specified addresses and conducted interviews to the full extent.

Table 1: Overview of the questioning process

Conducted interviews	1,010
Visited addresses	5,371
Repeat visits	1,625
No target group members in the family	401
No contact	2,466
A person from target group not at home	45
Contact refused	476
Target person refused to be interviewed	973

As the survey was an omnibus survey, the refusal to be interviewed cannot be explained by the fact that people did not want to discuss the topic of privacy and that the number of refusals somehow reflects people's attitude towards the subject matter. Reasons for refusal lay probably somewhere else – unsuitable time, time-consuming nature of the survey due to its extensiveness, and so on.

The survey data was processed with the SPSS 11.5 data processing programme and later analysed in the Institute of Social Studies of the University of Tartu with the SPSS 20 data processing programme. After the end of the survey, the sociodemographic composition of the respondents was compared to the sample requirements; to balance losses, data were weighted so that they would correspond to the theoretical model. The sex, age and region of respondents were taken into account in the weighting.

Of the whole database, **respondents in the 15-74 age group** were analysed as the target group of the survey. 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; the percentage error did not exceed 3.09%. A more detailed overview of the respondents is included in Table 2.

Table 2: Sample description

	Number of respondents	% of sample
Sex		
Female	500	52
Male	459	48
Age		
15–24	141	15
25–34	189	20
35–49	246	26
50–64	256	27
65–74	127	13
Nationality		
Estonian	655	68
Other	304	32
Education		
Elementary or basic education	159	17
Vocational, secondary, vocational secondary education	555	58
Higher education	245	26
Region		
Tallinn	299	31
Northern Estonia	159	17
East Viru County	111	12
Western Estonia	108	11
Central Estonia	71	7
Southern Estonia	211	22
Income per family member		
Up to €200	59	6
€201–€300	105	11
€301–€400	215	22
€401–€500	93	10
€501–€650	85	9
€651+	116	12
Marital status		
Married, in a partnership	525	55
Divorced, separated	122	13
Widowed	68	7
Single	243	25
Social status		
Entrepreneur, manager, top specialist	179	19
Mid-level specialist	219	23
Skilled worker, operator	153	16
Other, employed	56	6
Pupil, student	84	9
Pensioner	188	20
Other unemployed	80	8

OVERVIEW OF DIGITAL MEDIA USE AMONG ESTONIANS

As the study focuses on everyday information and communication technologies, we would like to give a short overview next to the sample description of what the habits of Estonians are in relation to technology use based on the results of the survey. In the past month, 83% of the people we questioned had used the Internet (72% on the same day or the day before, 9% within the past week, 2% within the past month). According to the Statistics Office data from the first quarter of 2014, 84% of Estonians had used the Internet (Infotehnoloogia leibkonnas: IT32...2014); therefore, the results are comparable. 3% of respondents said that they had been using the Internet before, but did not use it anymore, and 13% claimed not to have ever had any contact with the Internet. The most active age group were youngsters, as was to be expected:

- among 16–24-year-olds[1] 100% use the Internet (99.5% in the Statistics Office survey),
- among 25–34-year-olds it's 99% (98.8% in the Statistics Office survey),
- among 35–49-year-olds it's 93% (96.1% among 35–44-year-olds in the Statistics Office survey),
- among 50–64-year-olds it's 72% (86.4% among 45–54-year-olds and 70.1% among 55–64-year-olds in the Statistics Office survey),
- among 65–74-year-olds it's 39% (44.4% in the Statistics Office survey).

The Internet is mostly accessed via laptops and PCs, while half of Internet users access the web with a smart phone (Figure 1).

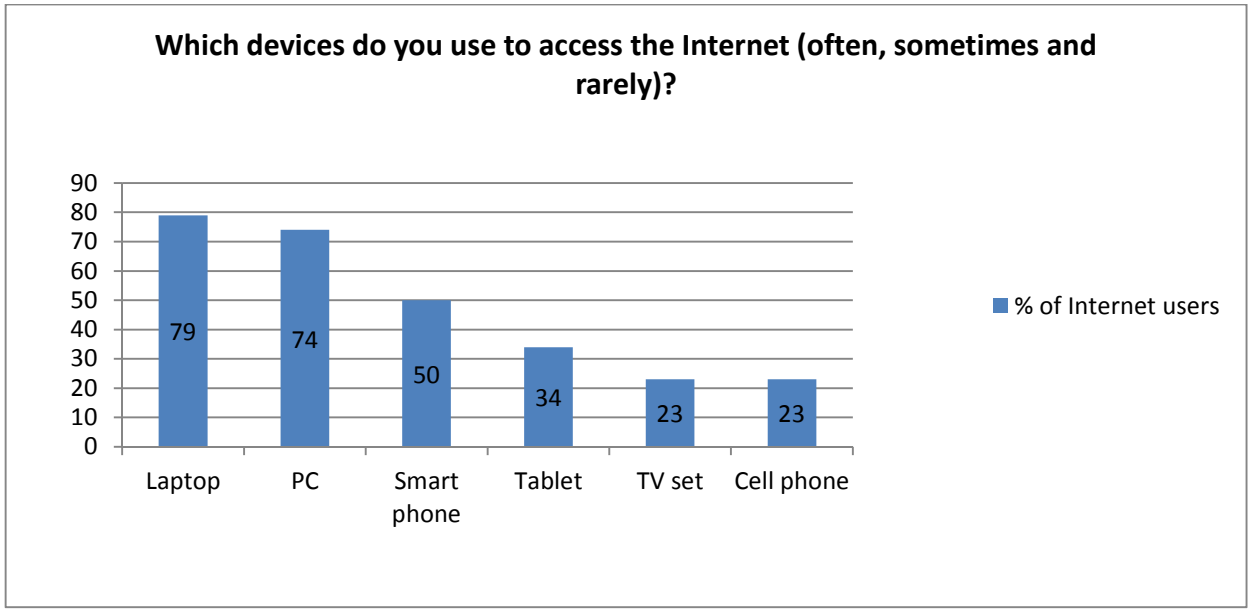

Figure 1: Devices used by respondents to access the Internet (n=799)

[1] We added up the responses to the question "When was the last time you used the Internet?" – "today, yesterday", "within past week" and "within past month". We did not count as Internet users the 1% of people who said that they had used the Internet a few months ago; in case of such a long gap we cannot really speak of actual Internet usage.

Figure 2 shows that even though we call everyone in general an Internet user, people actually spend their time on the Internet on a multitude of different activities. The largest share of people has used the Internet to consume media and to communicate (9% and 16% of respondents respectively do not use the Internet for these purposes), but the results for other activities vary more.

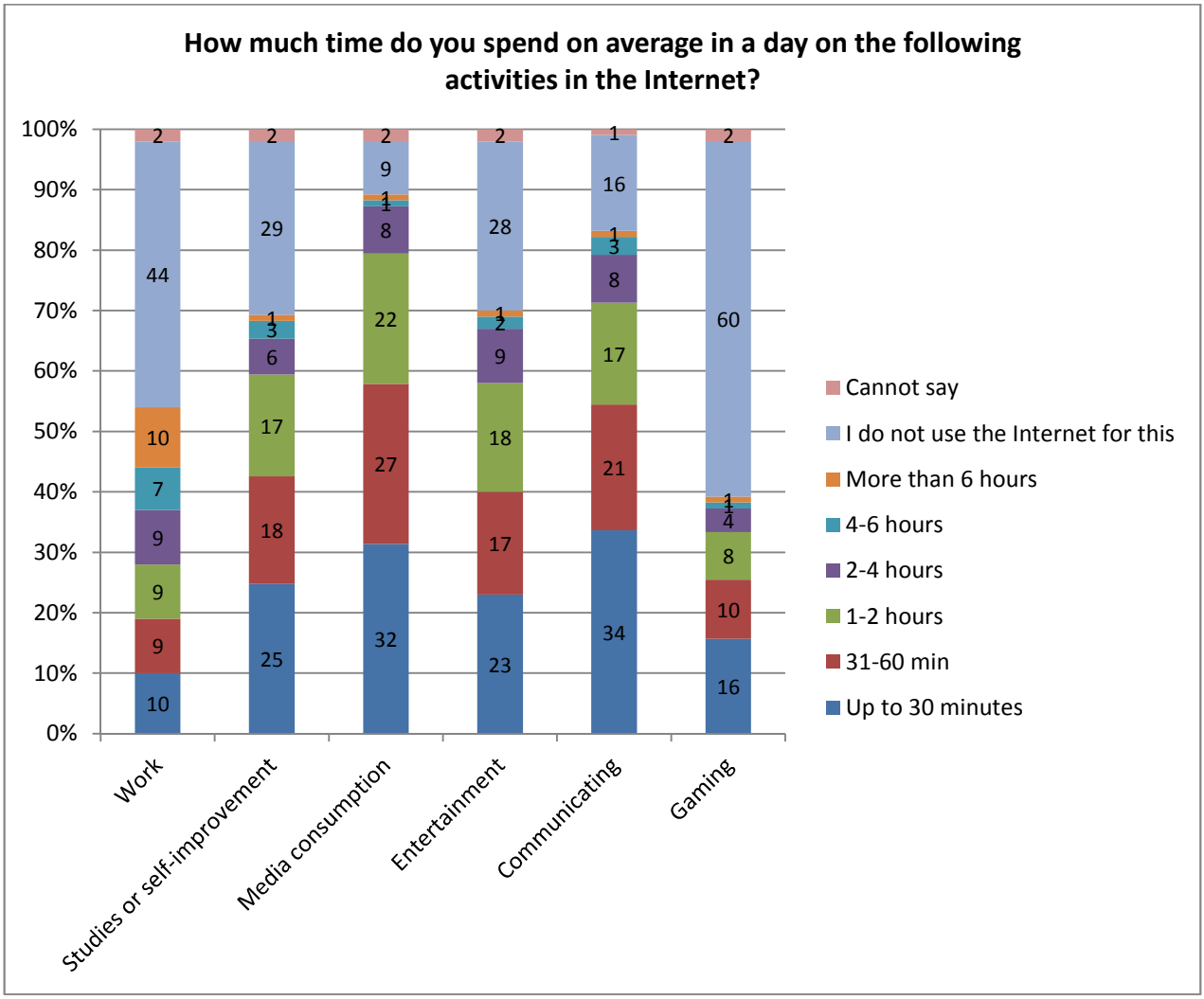

Figure 2: Time spent on the Internet by activity (% of Internet users, n=799)

Different experiences on the Internet certainly result in different opinions on privacy, as the outcome of the questionnaire as well as earlier studies show that the less experience and contact one has had with a topic, the more conservative and critical is one's attitude.

In generalising according to people's Internet use frequency and variety of activities,[2] it is possible to define three types of users: a non-user, an active user (does a lot of activities, spends a lot of time) and a moderate user (fewer activities, less time). In the case of Internet users, we can clearly see the differences in the time spent on various activities on average; the largest discrepancy is evident in time spent on entertainment (Figure 3).

[2] We conducted a two-step cluster analysis in which we firstly formed six clusters on the basis of the frequency and variety of activities and then grouped the clusters. The suitability of a six-cluster solution was based on an earlier theory (Kalmus, Keller & Pruulmann-Vengerfeldt 2009, Pruulmann-Vengerfeldt 2006)

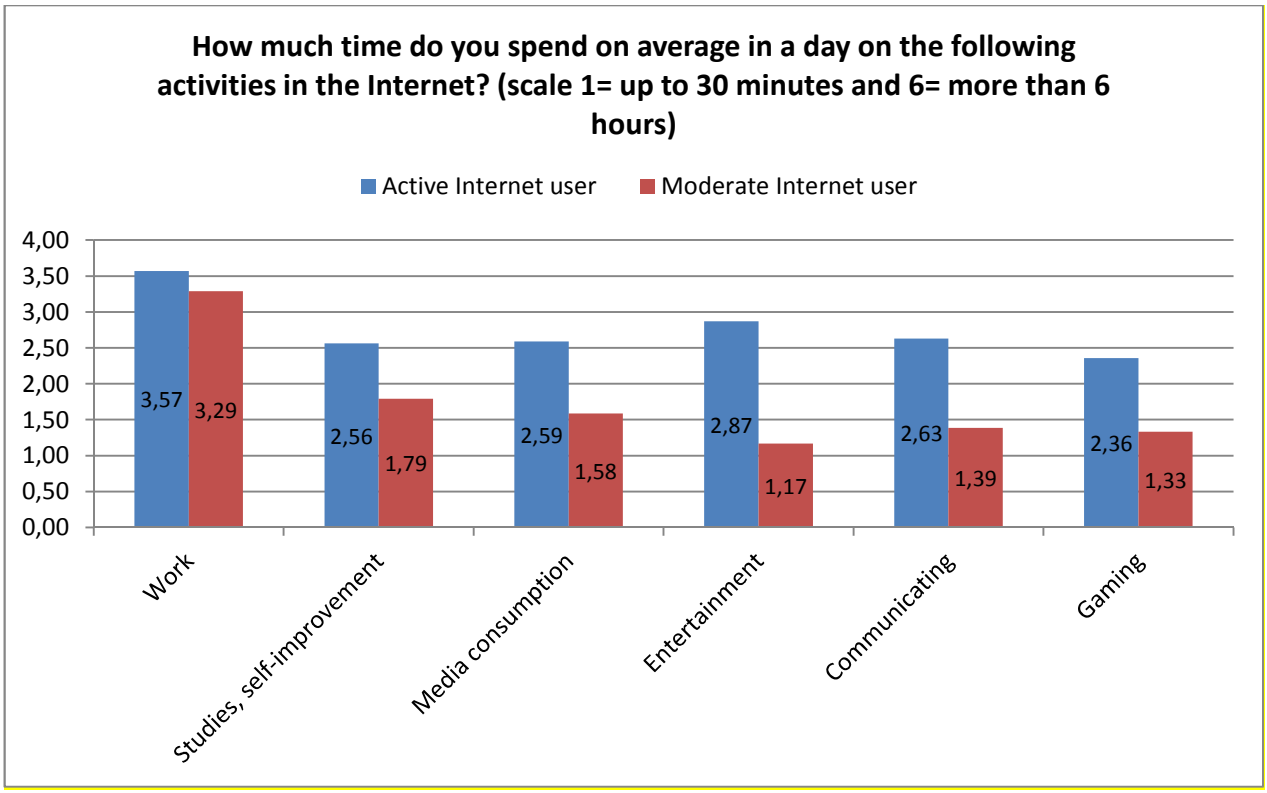

Figure 3: Differences in time spent on various activities on average by active Internet users and moderate Internet users (n=799)

Currently, a lot of the activities on the Internet are related to social networks, and this is also where people commonly come across situations that could be perceived as a threat to privacy. Therefore, we asked people to say which of the listed claims described their social media use most accurately, giving them five options, three of which were related to the activity level – active creator/consumer of content, moderate creator of content and lurker (Andrews 2003) – and two to non-use ("I have an account, which I haven't used in a while" and "I don't have an account").

72% of responding Internet users claimed to have a social media account and 66% use their account, which is considerably more than a few years ago – in 2012 only 56% of Estonians said that they used social media for communication (Eurostat news release...2012). On the other hand, according to the data on the first quarter of this year as collected by the Statistics Office, 60% of Internet users used social media (Infotehnoloogia leibkonnas: IT38...2014); the lower indicator could be due to the fact that social media use was only one of the many listed activities carried out on the Internet in that study, but the question in our study concerned this activity specifically.

51% of Internet users who participated in our survey create their own social media content, 15% act as lurkers, 6% have an account but have not used it for a while and 2% could not answer the question (Figure 4). As was to be expected, the biggest share of active social media users can be found in the youngest age group and, as the age rises, activity decreases: 81% of 15-24-year-olds use social media and create content (actively or moderately); for 25-34-year-olds it's 60%, for 35-49-year-olds it's 47%, for 50-64-year-olds it's 29% and for 65-74-year-olds it's 27%.

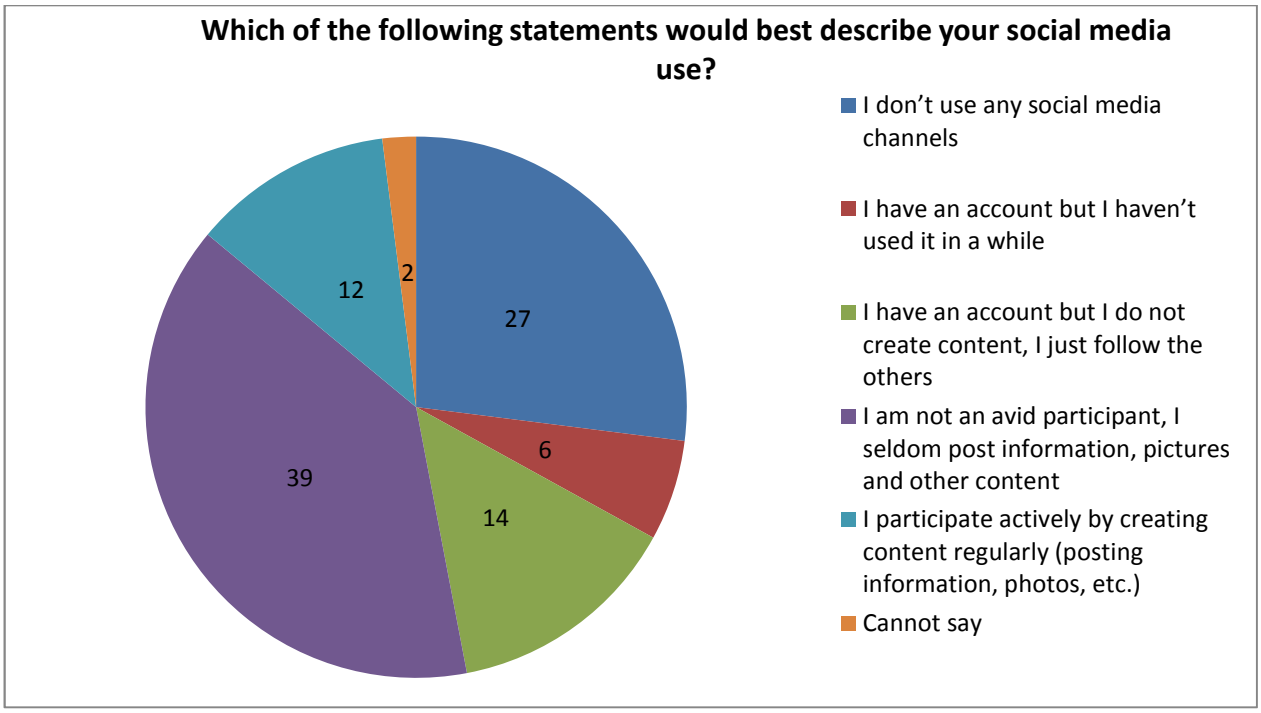

Figure 4: Ways in which social media is used (% of Internet users, n=799)

Varied participation in social media shows that even if people primarily link potentially privacy-invading situations to social media use, they have also developed passive privacy protection strategies to handle the participatory surveillance in social media (Albrechtslund 2008) – they monitor others and create limited content. Several researchers have stated that in online environments, the strategies that are based on minimum content creation and users' activity level have a negative side, too – to maintain and develop friendships, one needs to disclose personal information (Marwick, Murgia-Diaz & Palfrey 2010, Larsen 2007). It is naturally possible that a certain share of respondents do not use social media to maintain friendships, these environments have a different function for them.

It is also possible that the cause of moderate use is insecurity, which comes from insufficient skills in using social media environments. Estonian social media users are more likely to modify the privacy settings of social media environments to their requirements in comparison to the EU average (60% in Estonia, 51% in the EU), but at the same time they admit more frequently that they do not know where to find the terms of privacy and use of services or that such terms and conditions even exist (Special Eurobarometer 359... 2011).

EXPERT FOCUS GROUPS

In order to garner constructive criticism, valuable comments and supplemental information in relation to the study, we organised two expert focus groups in May 2014 and October 2014. Experts included specialists from different fields and sectors who come in contact with the topics of technology, privacy and data protection in their work. Both focus groups lasted for approximately two hours and were moderated by one of the authors of the study – the media studies professor Pille Pruulmann-Vengerfeldt from Tartu University.

The objective of the first focus group was to prepare the questionnaire so that it would fit the purpose and cover all relevant aspects. The following experts were involved:

- Kristi Kivilo – director of the Vaata Maailma SA foundation, one of the administrators of the project NutiKaitse 2017
- Mart Nutt – member of the supervisory board of the Estonian Institute of Human Rights
- Merili Oja – advisor in the Public Law Division of the Legislative Policy Department of the Ministry of Justice
- Silver Sarapuu – advisor in the Data Protection Inspectorate
- Liisa Tallinn – then communication manager of the Information System Authority

Greatly valued comments were received by e-mail from the following experts:

- Mait Heidelberg – advisor in the Ministry of Economic Affairs and Communications
- Ülle Madise – constitutional law professor in the Chair of Constitutional and Administrative Law of the Faculty of Law of Tartu University, legal advisor to the President of the Republic
- Katrin Merike Nyman-Metcalf – head of the Chair of Law and Technology of Tallinn Law School of Tallinn University of Technology, expert on international law

The second focus group concentrated on the preliminary discussion of the study results. The following experts participated:

- Kristi Kivilo – director of the Vaata Maailma SA foundation, one of the administrators of the project NutiKaitse 2017
- Hans Lõugas – technology journalist of the *Eesti Päevaleht*
- Mart Nutt – member of the supervisory board of the Estonian Institute of Human Rights
- Katrin Merike Nyman-Metcalf – head of the Chair of Law and Technology of Tallinn Law School of Tallinn University of Technology, expert on international law
- Merili Oja – advisor in the Public Law Division of the Legislative Policy Department of the Ministry of Justice
- Piret Pernik – research fellow at the International Centre for Defence Studies, specialist on cyber security
- Silver Sarapuu – advisor in the Data Protection Inspectorate
- Marek Tiits – chairman of the management board of the Institute of Baltic Studies, one of the administrators in the project "*Fast and trustworthy identity delivery and check with e-passports leveraging traveller privacy*" (coordinator of the social, legal and ethical package)
- Siim Tuisk – third sector activist (concerned with the topics of Internet freedom and rights)
- Anto Veldre – expert of information security in the Incident Response Department of the Information System Authority, free thinker

The discussion of the second focus group has been used below, in the presentation of results, to illustrate the outcomes with clarifications and recommendations from the abovementioned experts. We would hereby like to thank all the experts who participated in the focus groups – thanks to you, the study became much more informative and comprehensible.

STUDY RESULTS

Below, we will present the results of the study under the following umbrella questions: who do Estonians trust in matters of privacy and who do they not? What kinds of situations disturb people? Who should protect people's rights to privacy? How would it even be possible to protect people's privacy? We will start the chapter with an overview of the results and by mapping people's general attitudes.

***Technology journalist Hans Lõugas**: "I think that people here have in mind the photos and information posted in Facebook. But data uploaded on the Internet could also include the back-up of phone data on the web. I believe that if people had considered this, they would have answered differently."*

As many as 53% of respondents agreed to the claim that "the data that I have entered on the Internet can be freely used by anyone", and this serves as proof that the Internet is largely seen as a public place. This publicness differs from the classic publicness (boyd 2007) as the data is permanent, searchable, replicable and available to the invisible audience. This could indicate one of the problems related to awareness – by replying that data can be used by "anyone", people can only imagine a limited potential audience (Siibak & Murumaa 2011) and never all of the interested parties.

Of the respondents, 18% thought that their knowledge about what kind of data was collected on them was good or extensive, 36% claimed it was satisfactory and 43% considered it insufficient or completely lacking (Figure 5). Age-wise, the oldest people assess their knowledge to be the most limited – 65% of people at the age of 65-74 found that their knowledge is insufficient or non-existent.

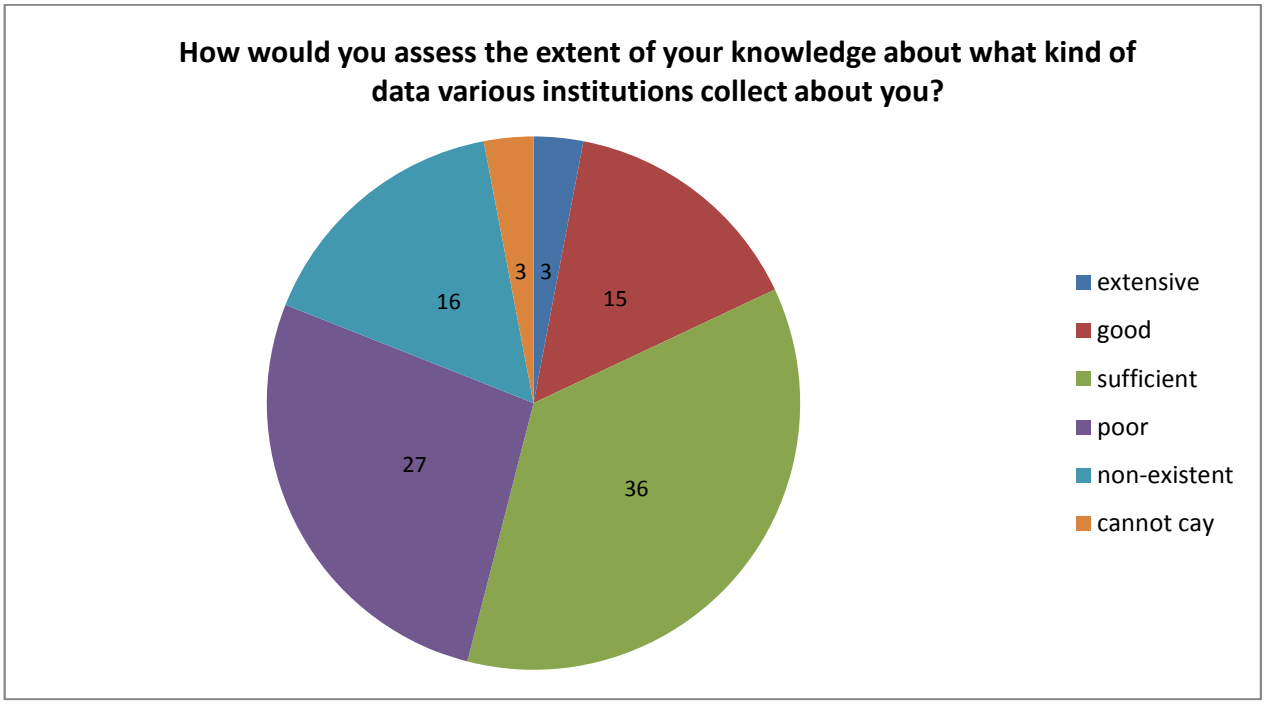

Figure 5: How do people themselves assess their awareness of data collecting (% of all respondents, n=959)

In accordance with expectations, the least knowledge is claimed by non-users of the Internet – 36% of them said that they had no idea about what kind of data different institutions collected on them; among the moderate users, this response was given in 17% of the cases and among active web users in 7% of the cases (Figure 6).

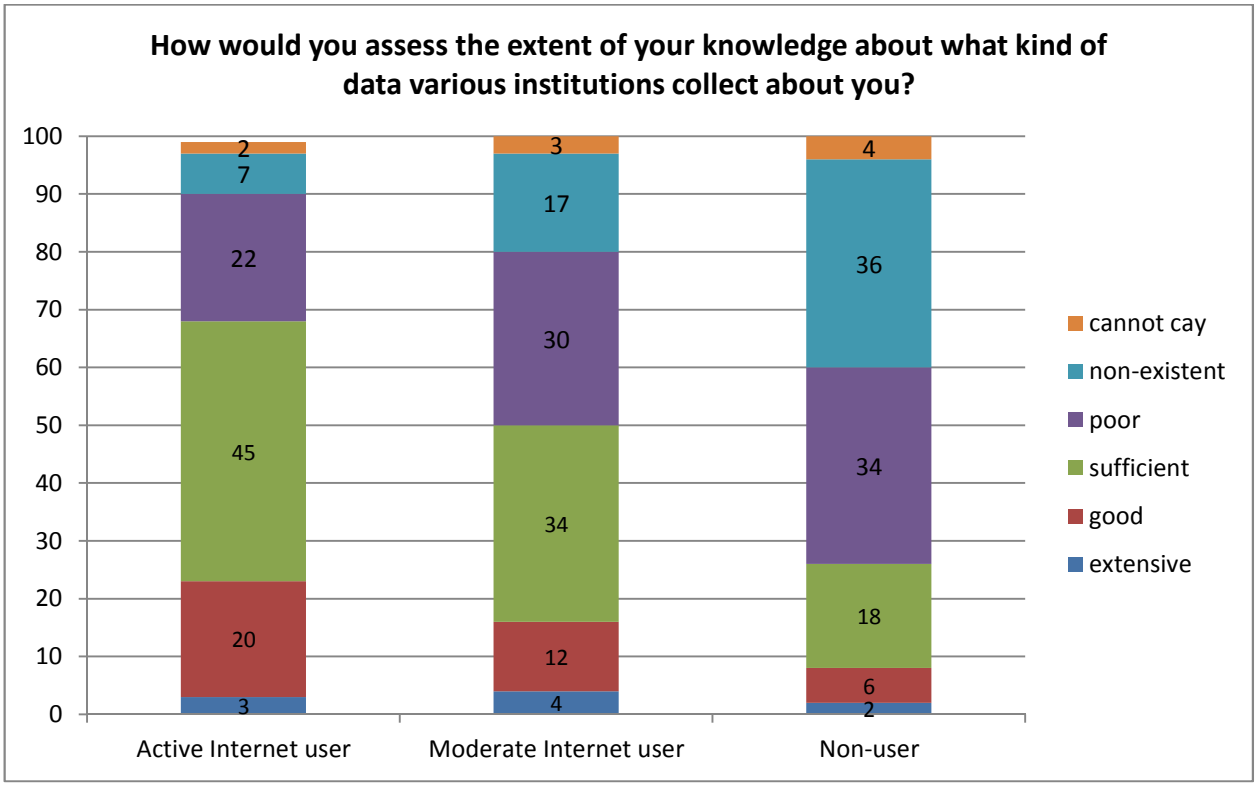

Figure 6: Self-proclaimed level of awareness of personal data collection among different respondent types according to Internet use frequency (% of all respondents, n=959)

We also tried to ascertain what the general points of view of Estonians are on the right to privacy (Figure 7). The majority of respondents (53%) are of the opinion that being worried about personal data is relevant (the last claim on the Figure). However, the share of people who find that the whole issue has been exaggerated is also significant – 41%.

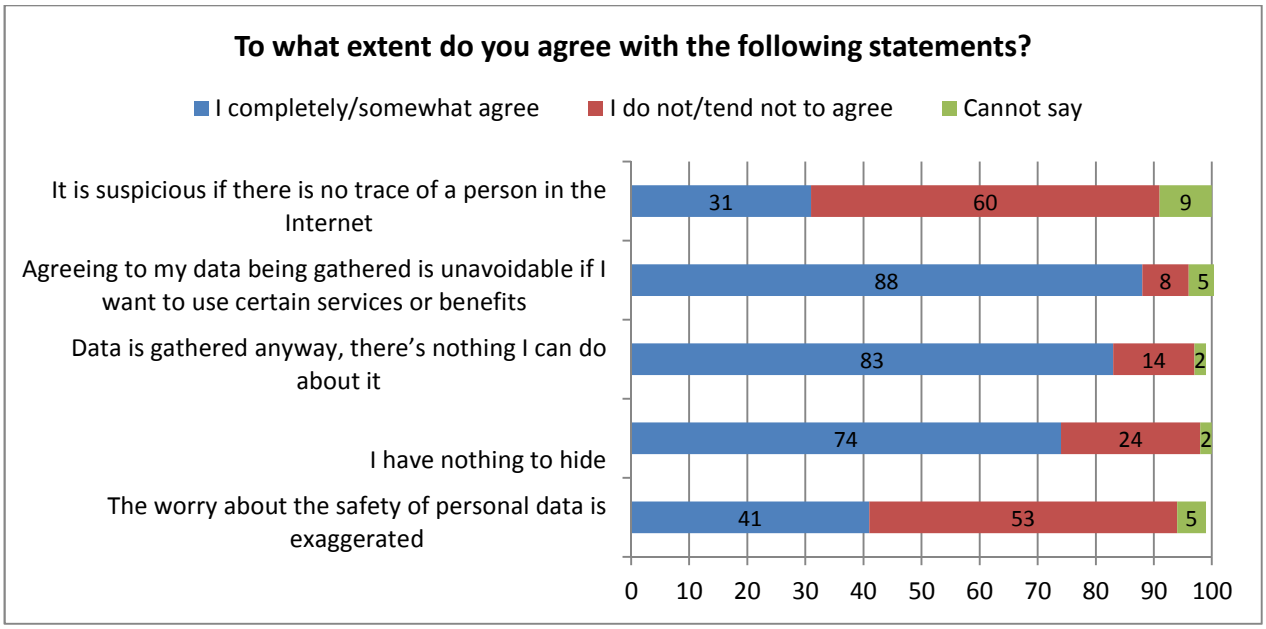

Figure 7: To what extent do people agree to the claims about accepting the inevitability of the loss of privacy (% of all respondents, n=959)

In connection to that question, we analysed whether very active and extremely non-active web users are somehow more worried than the average user. We wanted to determine if we could see a normal distribution based on the working hypothesis derived from the technology acceptance model (people with high user activity and awareness are worried because they are familiar with how privacy can be invaded; people with low or non-existent user activity and awareness are worried because they are conservative and sceptical of innovations). To our surprise, the results of this study did not confirm to the hypothesis – the indicators were similar in both groups.

Third sector activist Siim Tuisk: *"The common opinion that young people are not worried about their privacy definitely does not hold."*

Age-wise, it can be noted that younger people view the protection of personal data as a bit more important than other age groups: 58% of 15-24-year-olds consider it relevant to be worried about the protection of personal data (the rest of the indicators are rather similar: 39% of 25-34-year-olds, 41% of 35-49-year-olds, 45% of 50-64-year-olds and 46% of 65-74-year-olds find the same).

Figure 8 indicates that the two youngest age groups (the age group of 25-34-year-olds particularly stands out) feel a bit less that the collecting of data is inevitable, which could mean that younger people sense their role as a more active one. Frequently, young people are the first to accept technological innovations and, therefore, any problems they notice or perceive could be indicators of problems rearing their head in society at large (Livingstone & Haddon 2009, Miles 2003). The fact that young people consider the worry about the protection of personal data relevant more often than other age groups and sense that the collection of data is inevitable less often shows us that the common misconception that young people care less about their privacy is unfounded.

Nevertheless, we can see that the majority of people accept the situation – a sort of fatalist attitude, which became evident in the Eurobarometer privacy survey (Special Eurobarometer 359... 2011).

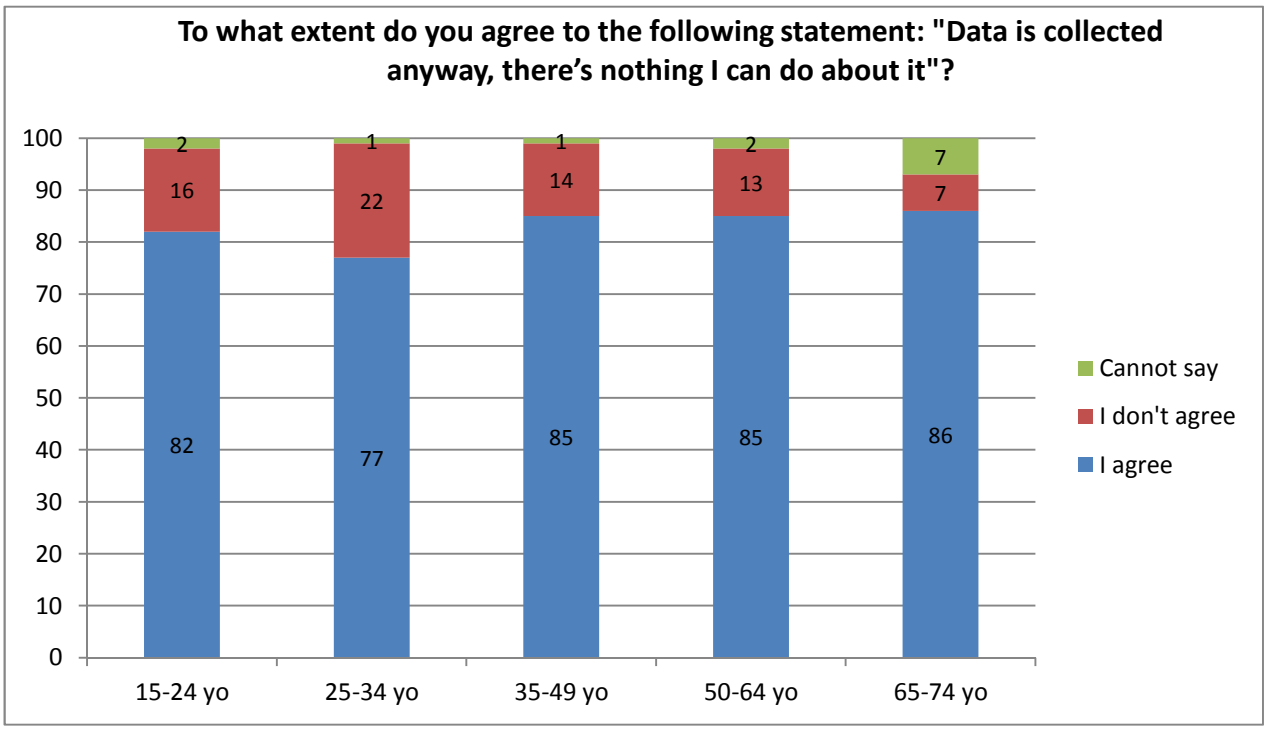

Figure 8: To what extent do different age groups agree to the statement about the perceived inevitability of data collecting (% of all respondents, n=959)

Younger age groups include more people who agree to the statement that it is suspicious if there are no traces of a person on the Internet (45% of 15-24-year-olds, 32% of 25-49-year-olds, 24% of 50-64-year-olds and 21% of 65-74-year-olds); however, we should pay attention to the fact that as many or more people thought that it was not suspicious if the digital trace was missing.

We see that on the one hand a large part of people think that it is important to be worried about the protection of personal data; however, in the case of data sharing they mention inevitability and do not sense the potential sensitivity of their own data – 74% of respondents agreed to the claim that "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). Greater influence in terms of this claim is exerted to the extremes of replies (I completely agree, I completely disagree) according to Internet use frequency as a factor (Figure 9), which means that non-Internet users more often agree completely and active Internet users more often disagree completely.

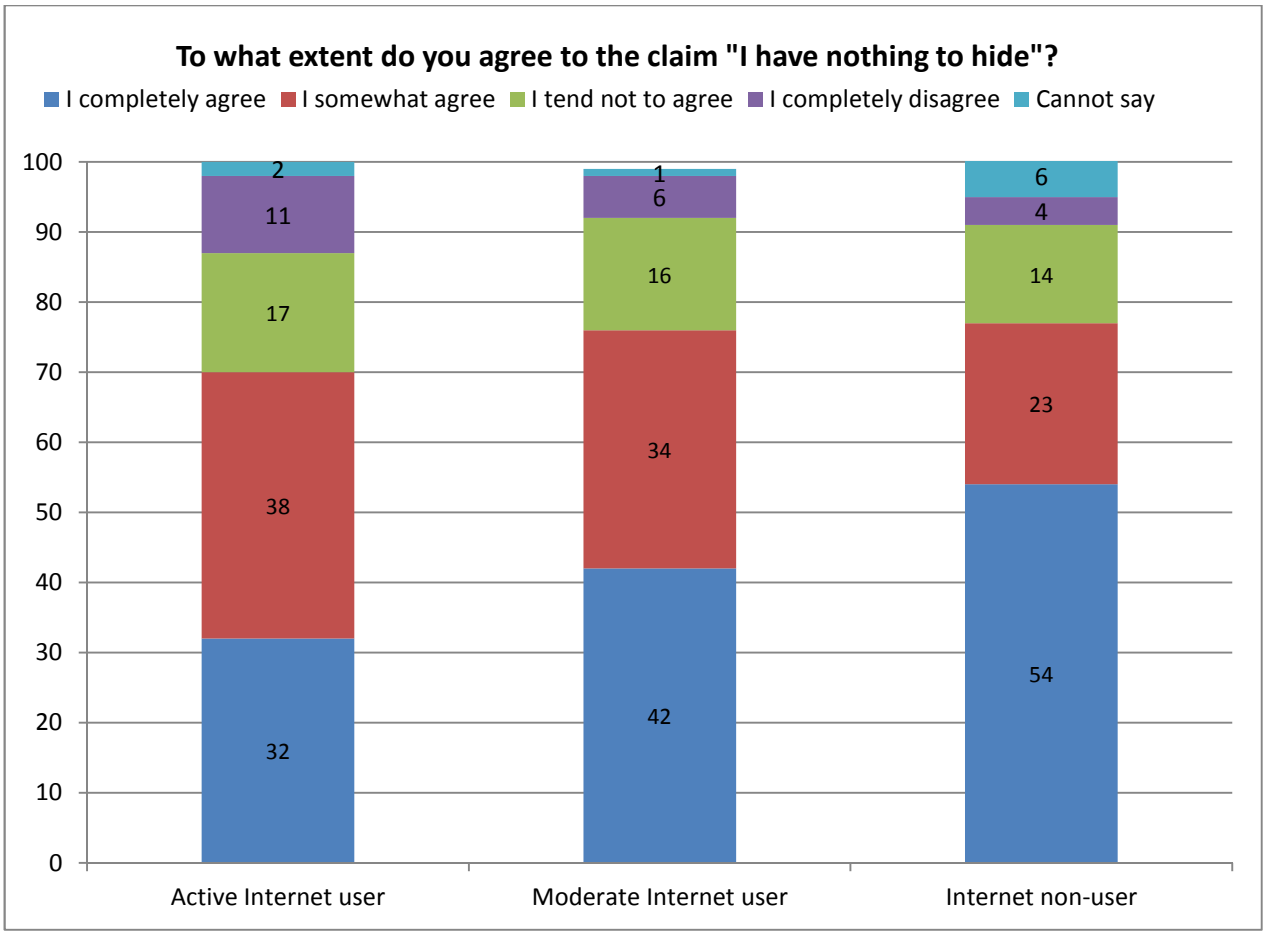

Figure 9: Influence of the active Internet use level on the responses to the claim that "I have nothing to hide" (% of all respondents, n=959)

Mart Nutt, Estonian Institute of Human Rights: *"We should be wary of claims that the time for privacy is over and that this topic does not need to be covered anymore. Privacy is a presumption for the protection of many other human rights."*

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 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. If the state or large corporations ignore the right to privacy through their continued activities and with the help of their greater power (the NSA incident), 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.

WHO IS TRUSTED, WHO ISN'T?

In the questionnaire, we listed situations that could be treated as potential risks to privacy and asked the respondents to say whether these situations threaten people's privacy or not. The described examples were chosen to examine the perceptions of the actions of participants from different sectors (e.g., in the case of monitoring people and collecting information on them if this is done by the state, other countries, employers, financial institutions, private enterprises (smart device applications were mentioned separately), acquaintances or strangers). Figure 10 indicates that the majority of respondents find that all potential risks could endanger people's privacy (60-72% agreement rate regarding different claims).

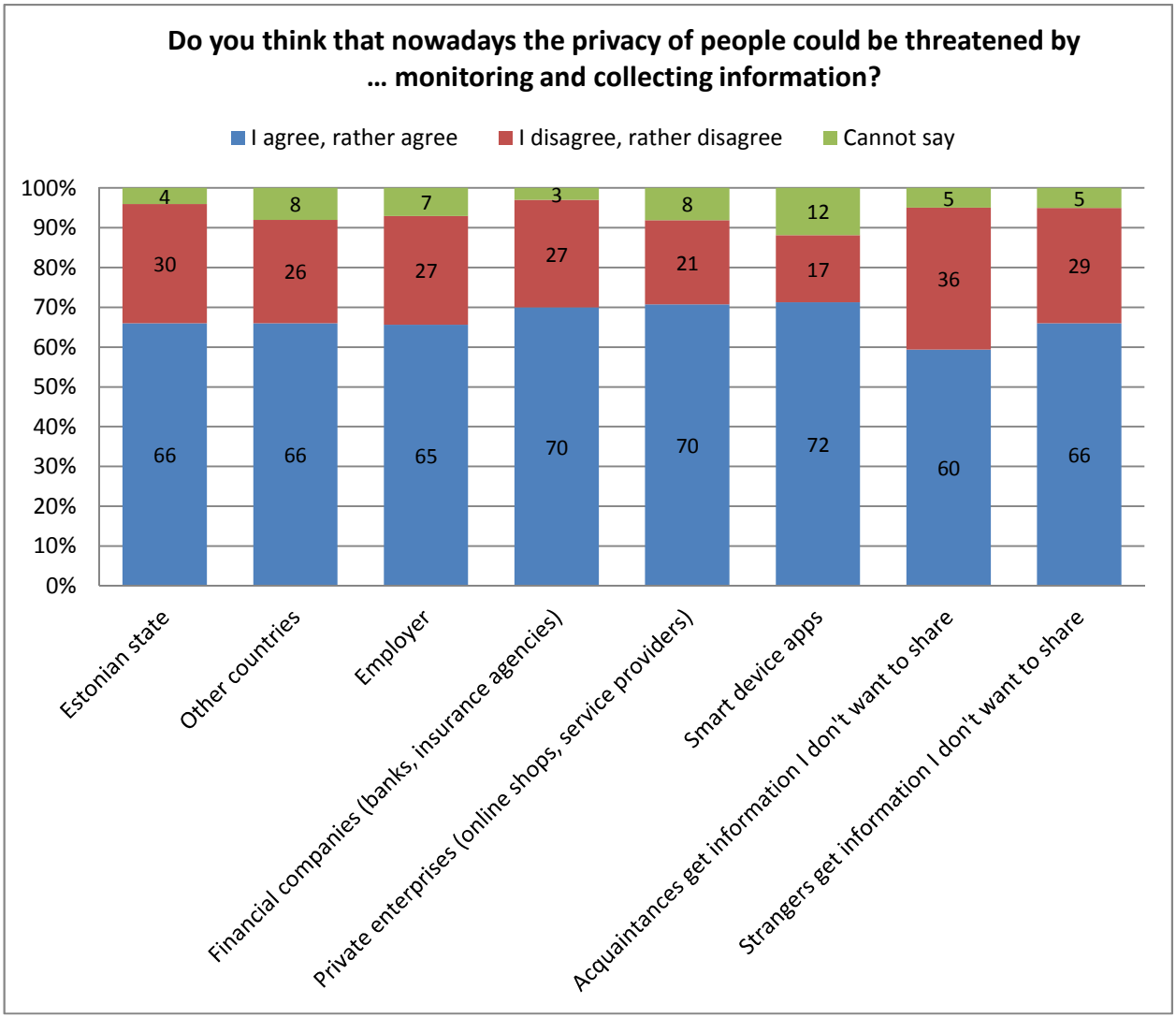

Figure 10: To what extent are different parties perceived as threats to privacy (% of respondents, n=959)

People find the biggest threat 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 monitoring and collecting information that a person does not wish to share. A person's social media image is in actuality often a collective creation. Every day, we trust personal information to people in our networks, assuming that they share our standards on privacy and socially acceptable behaviour.

> ***Piret Pernik, research fellow at the International Centre for Defence Studies:*** *"People trust medical institutions, who collect the most private information. Then again, they do not trust service providers, although – come to think of it – what kind of information do they collect, then?"*

Additionally, we asked people to what extent they trusted different institutions in respect of the purposeful use of their data or as protectors of their data. Figure 11 summarises assessments about authorities and institutions in the public sector, and Figure 12 concerns the representatives of the private sector – in this way, it is easier to compare people's opinions on data use and protection. The study results confirm that the public and private sectors should be distinguished because people tend to trust the former one more than the latter.

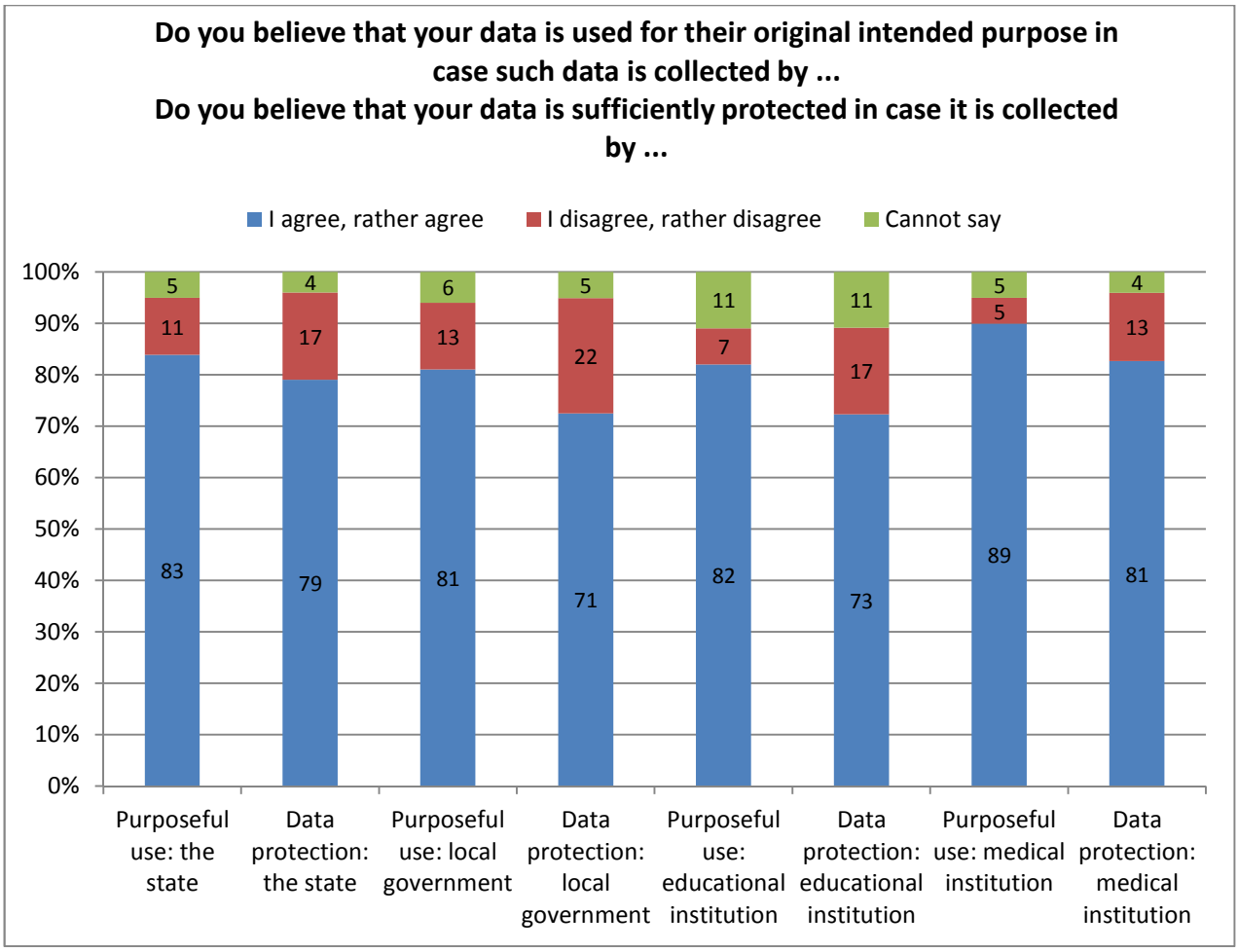

Figure 11: To what extent are public organisations trusted in terms of the purposeful use and protection of data (% of respondents, n=959)

All listed institutions in the questionnaire were trusted a bit more as purposeful users of data than as protectors of data (Figure 11, Figure 12). One of the reasons for this might be the visibility of the topic – subject matter included in public discussions is adopted into personal assessments. In recent years, the media has covered many cases of information leaks, which have raised awareness of the topic among citizens.

Therefore, we could see on Figure 11 that the trust in data use and protection is the greatest in case of medical institutions (89% trust them as purposeful data users, 81% trust them as data protectors), then comes the state as a generalised institution (83% and 79% respectively), while trust is also high in case of educational institutions (82% and 73% respectively) and local governments (81% and 71% respectively). Trust in purposeful data use and data protection was lowest among the respondents in terms of private enterprises (such as e-stores) (48% and 31% respectively); Internet service providers were also held in low esteem (59% and 39% respectively).

People's trust is a little greater in the ability of financial institutions to use and protect people's data, and separately listed employers are also trusted more than private enterprises. The disclosure of financial data usually means actions related to everyday banking, which people might view as state business because of certain user and authentication functions, although in reality financial institutions are still part of the private sector. We have assigned the employer to the same position as a private enterprise, because even though an employer can be a public sector organisation, its relationship with the employee is a "transaction-based relationship" and we concluded that such a division would make sense.

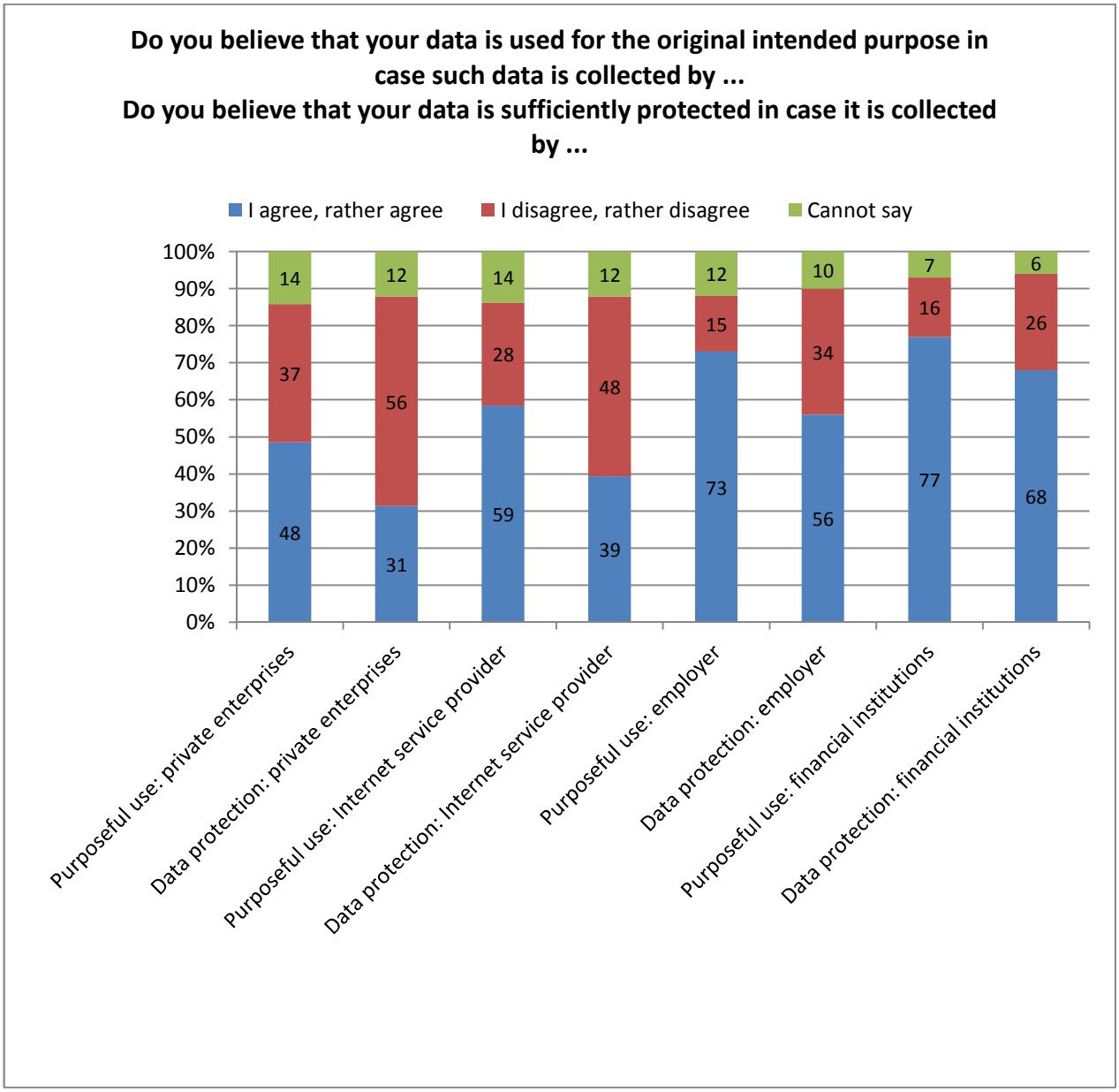

Figure 12: To what extent are private enterprises trusted in respect of the purposeful use and protection of data (% of respondents, n=959)

When we compare the relevant results of this study[3] to the results of the 2011 Eurobarometer on the same topic (Special Eurobarometer 359... 2011), we can see that trust rates generally correspond – all of them are a few percent lower at the moment (in respect of the state, medical institutions and private sector). Trust has decreased more in the case of communication services (49% on average in our study, 65% in the EU study) and financial institutions (72.5% in our study, 86% in the EU study), whereas one certainly has to factor in the structure of the studies and differences in questionnaires.

[3] Comparison included actors that were listed in both studies; the average of two indicators was calculated on the basis of the purposeful use and data protection percentages.

We asked people's opinions on unauthorised access to and collection of data, and based on the results we can see that the respondents consider the problem equally serious, whether the data is accessed without consent or collected by the state, enterprises or other people (Figure 13).

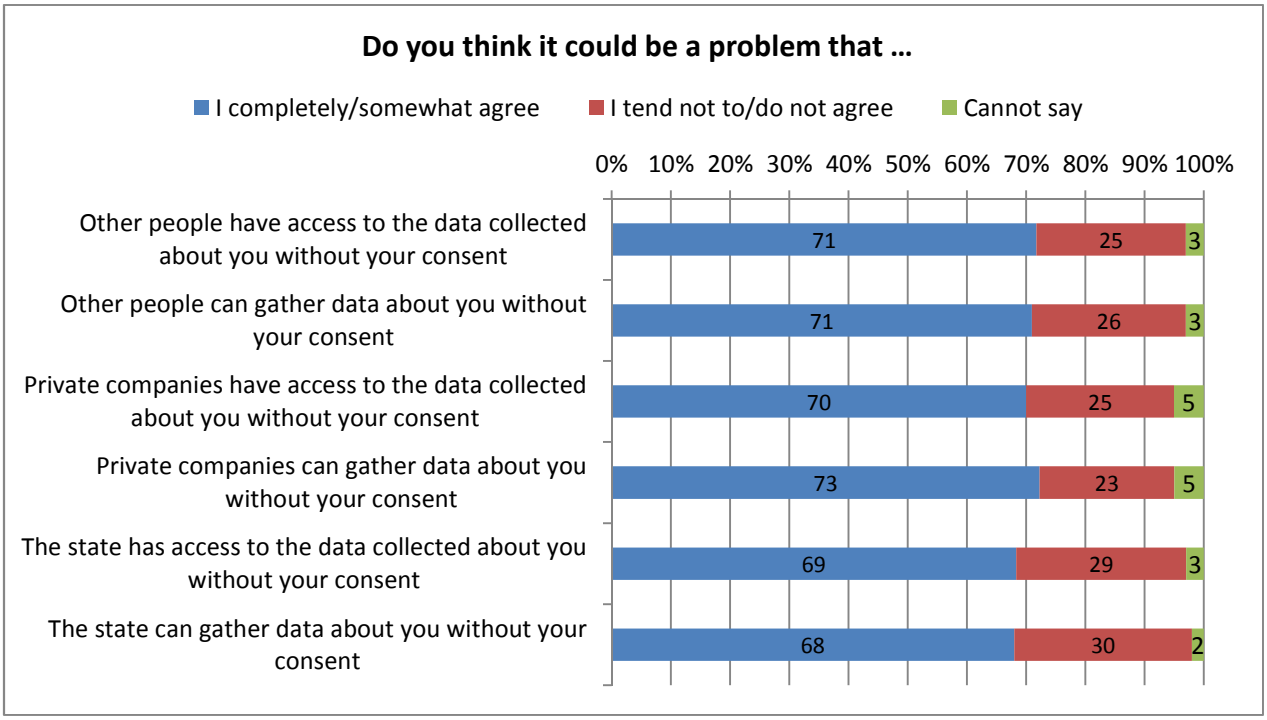

Figure 13: Unauthorised access to and collection of data perceived as a problem (% of all respondents, n=959)

> ***Katrin Merike Nyman-Metcalf, head of the Chair of Law and Technology of Tallinn University of Technology:*** *"When services become e-services, then security is more emphasised. When the information is on paper, then the importance of privacy is not stressed and people are less worried."*

We are currently dealing with a problematic situation as digitally stored data can be easily copied and transferred. Third sector and Internet freedom activist Siim Tuisk mentioned during the expert interview that "a person can physically carry about 50 kg of paper but, nowadays, it is possible to walk out the door with a whole national database without anyone noticing". The worry about privacy is related to topical issues – the agenda setting – hard-copy information can also endanger privacy but public debates mostly focus on digital data as a source of risk and the same view is adopted by people in general.

A controversy in comparison to earlier survey results is the following: the majority of questioned people (61%) were of the opinion that the state should, in general, have more rights to process personal data without consent in order to ensure security (Figure 14).

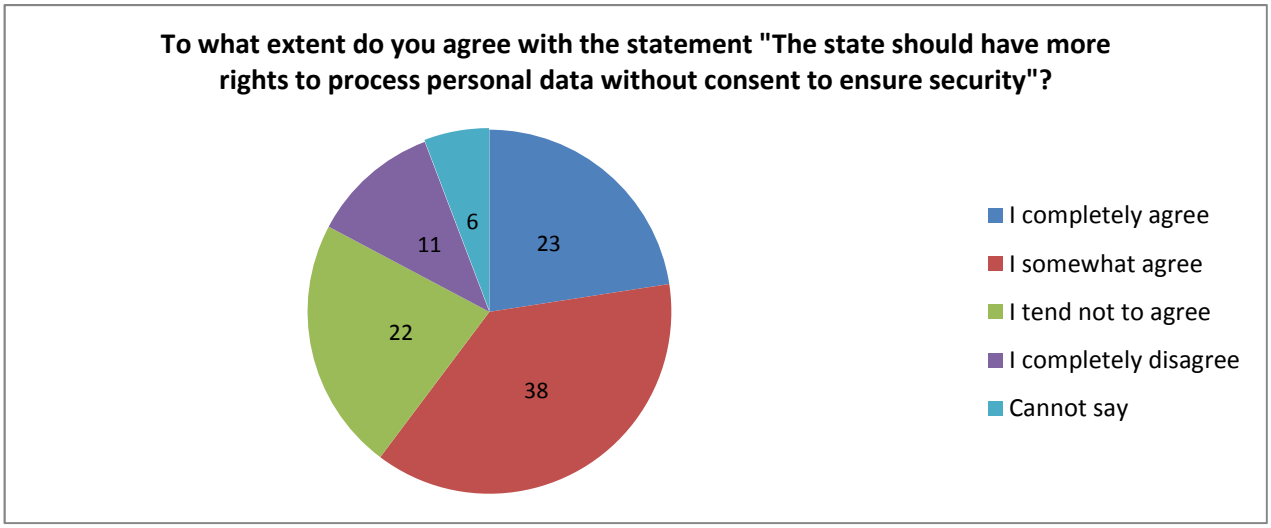

Figure 14: Agreement to security-related personal data processing (% of all respondents, n=959)

Katrin Merike Nyman-Metcalf, head of the Chair of Law and Technology of Tallinn University of Technology:
"People are aware that the information is out there and that if the state wanted to abuse it, it would be really easy in the information society. To date, there have been no problems. This way of thinking is not naive, but considered – the trade-off is acceptable. If people would find out something that would touch them personally, this situation would rapidly change."

This result surprised our experts, who noted that despite the keyword "security" in the question they would have expected, in the light of the NSA and Wikileaks scandals, people to be more sceptical. We must not forget that the perception of the right to privacy is extremely context-sensitive; in one situation (for instance, catching terrorists) the parties are allowed more than in another situation (e.g., evaluation of solvency or financial status on the basis of social media).

The high percentage of respondents who agree to the state's unauthorised access to its citizens' data serves as proof that Estonians share the positive attitude of the rest of Europe towards the supervisory and protective role of the government and state. In the United States, the results of a similar survey would probably differ, mainly because people are conscious of more scandals centred around the state's access to data without people's consent.

This leads us to the next sub-topic, in which we have tried to map Estonians' assessments of potentially privacy-violating situations through prescribed circumstances.

WHAT KINDS OF SITUATIONS BOTHER PEOPLE?

First, we asked general questions about some of the more common potentially privacy-invading situations and consequences. We wanted to know whether the respondent senses that people's privacy could nowadays be threatened by 1) the use of data for some other purpose than what it was originally collected for some other purpose than what it was originally collected (Figure 15)– it was considered a threat by 74%; 2) the interference of others into one's personal matters and freedom of choice on the basis of collected information (Figure 16) – it was considered a threat by 73%; 3) the combination of data available in order to find out things about a person, which the said person would like to keep a secret (Figure 17) – it was considered a threat by 84%; 4) identity thefts (Figure 18) – they were considered a threat by 81%. In the previous section we learned that trust in different institutions differs to a considerable extent, so it follows that data collection and processing are generally perceived as threats, but the threat is smaller in relation to certain institutions (for instance, people trust the medical system with their data).

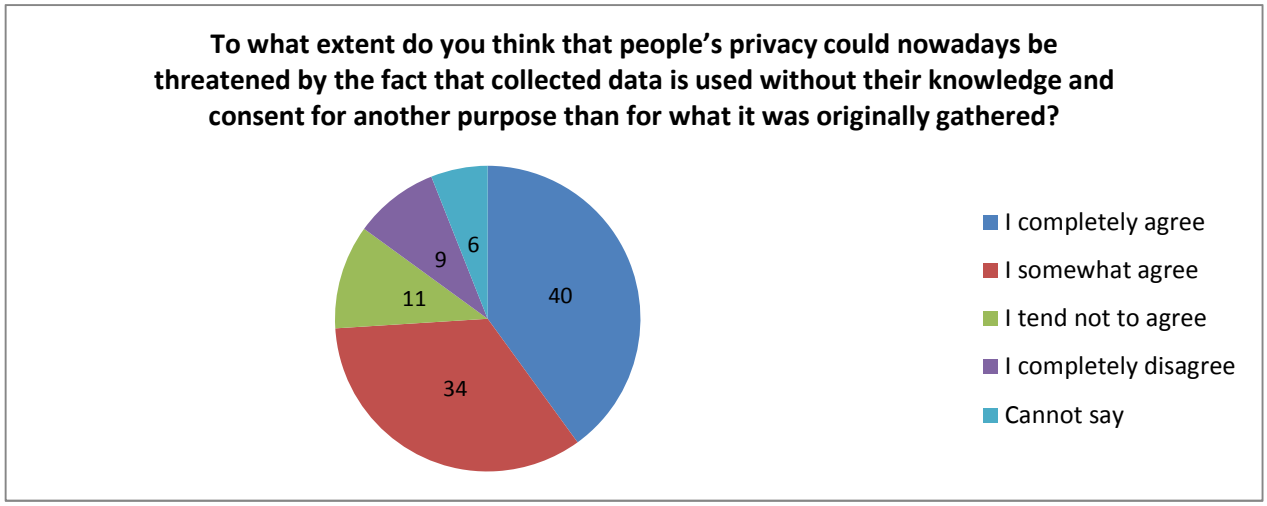

Figure 15: To what extent do people consider it a threat to privacy when data is used for a different purpose than for what it was collected (% of all respondents, n=959)

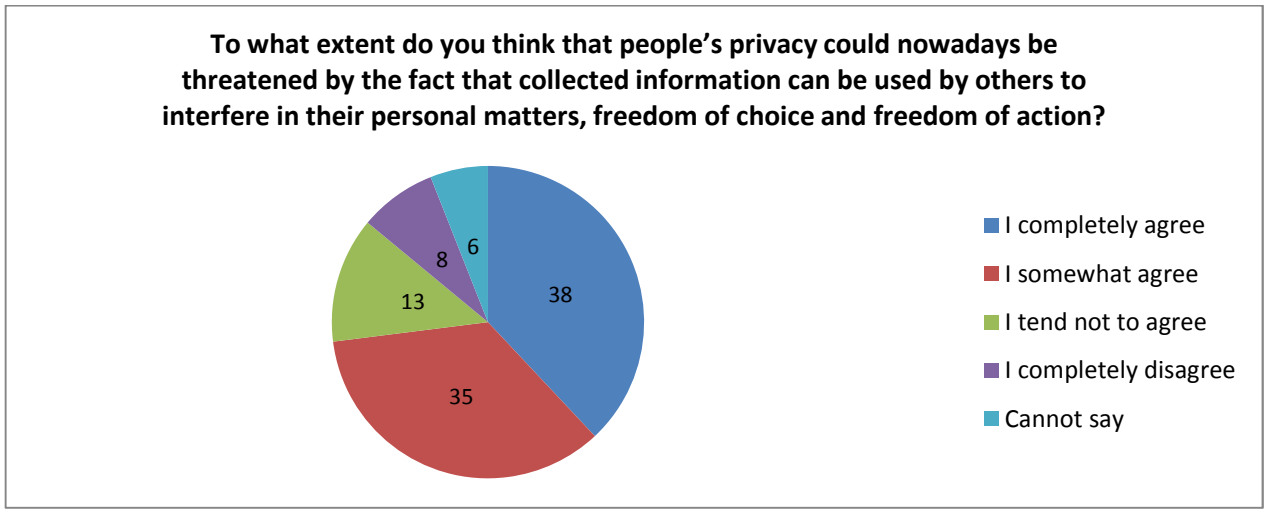

Figure 16: To what extent do people consider it a threat to privacy when information is used to interfere in other people's personal matters (% of all respondents, n=959)

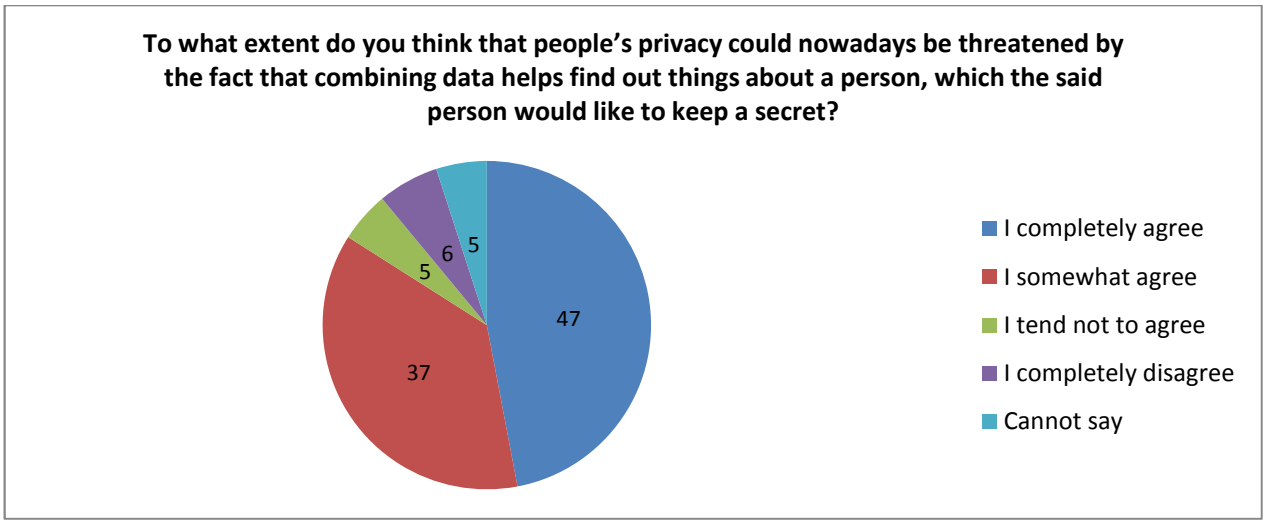

Figure 17: To what extent do people consider it a threat to privacy when data is combined to find out information that a person might not wish to disclose (% of all respondents, n=959)

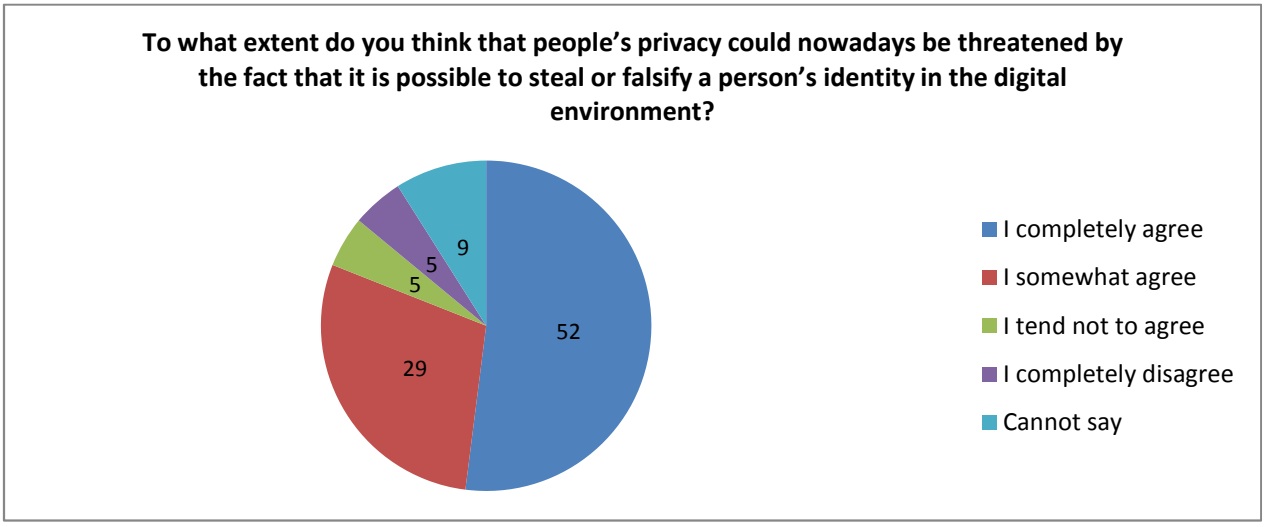

Figure 18: To what extent do people consider it a threat to privacy that in the digital environment it is possible to steal/falsify a person's identity (% of all respondents, n=959)

It is difficult to discuss privacy based on generalised claims; therefore, we decided to describe real-life contexts to people for ease of imagination. The questionnaire provided respondents with several sample situations in which we could ask about the violation of privacy in terms of the use of everyday technologies. It is not possible to envision all potential scenarios (and as is evident from Anto Veldre's comment below – only case-based awareness-raising is not efficient in the long run), but to explain the topic we considered it necessary to plant the issues related to the right to privacy in easily comprehensible daily situations.

> ***Anto Veldre, expert of information security in the Incident Response Department of the Information System Authority:*** *"The Devil is in the detail – the probability of all details coinciding is low but, should this happen, there is trouble. In several different ways. And to raise awareness we cannot tell people millions of examples to learn and remember."*

In total, 21 situations were presented to respondents in two questions (one to all respondents, one to Internet users). The situations described in the first question for everyone were such that the frequency of one's Internet use should not play a role:

1. In order to provide me with a loan, the bank analyses my payment history
2. In order to offer me a discount on products or services, my buying behaviour (including online commerce and web searches) is analysed
3. In order to ensure the safety of air traffic my travel behaviour and history are analysed
4. In order to provide me with better medical services, all my data is available to all doctors via an information system
5. Before hiring me, my employer checks the web for public information on me
6. In order to create a community spirit, the kindergarten shows pictures of my child on its web page
7. In order to catch criminals, the police analyses my public and private data both in state databases and on social media
8. In order to ensure safety in the city and on roads, the police has security cameras in operation 24/7 to detect undesirable behaviour or dangerous situations
9. In order to give out means-tested benefits, the state analyses databases and publicly available information
10. In order to ensure the safety of schoolchildren, schools have security cameras
11. In order to engage in more open communication with pupils, a teacher follows their activities on Facebook

In the cases above, all respondents gave their answers, and from the Figure below we can see that 18% of them did not find any of the 11 potentially privacy-invading situations bothersome (Figure 19).

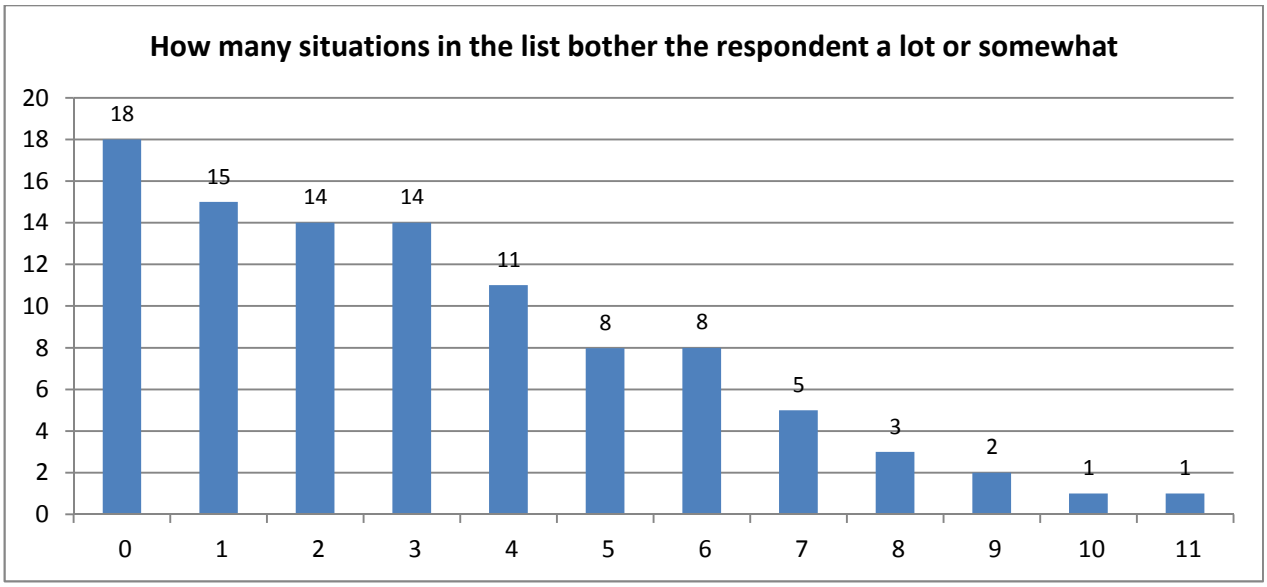

Figure 19: Summarised list of different situations that bother people (% of respondents, n=959)

The second question described situations and to understand these one needed to be an Internet user:

12. In order for the smart device to recommend the best restaurant or car park in the vicinity or to quickly find me a taxi, my location data is analysed
13. In order to efficiently offer me content that I might be interested in (e.g. in Google or YouTube), my general online behaviour is analysed
14. In order to suggest potential acquaintances for me, social networks (e.g., Facebook) analyse my network of friends and acquaintances
15. In order for me to revisit the history of a conversation, Skype records all my conversations
16. In order to ensure national security, the state requests access to my data from the Internet service provider
17. In order to spend quality time and play games, I give the applications in mobile and online environments access to my personal data
18. In order to target me with specific advertisements, e-mail service providers (e.g., Google, Yahoo, mail.ee) analyse the content of my e-mails
19. In order to get advice and support from other parents, I should disclose data on my child in a forum or blog dealing with family matters (e.g., Perekool)
20. In order to receive useful workout tips and gain followers, I should publish my workout data via workout applications or social media
21. In order to keep in touch with friends and maintain good relations with them, it is presumed that people can publish photos of me partying on the Internet

In case of this question, which was only answered by Internet users, 20% of respondents were not bothered by any of the ten specified situations, although the average level of being bothered was higher in this case (taking into account that described situations were also more private in nature) (Figure 20).

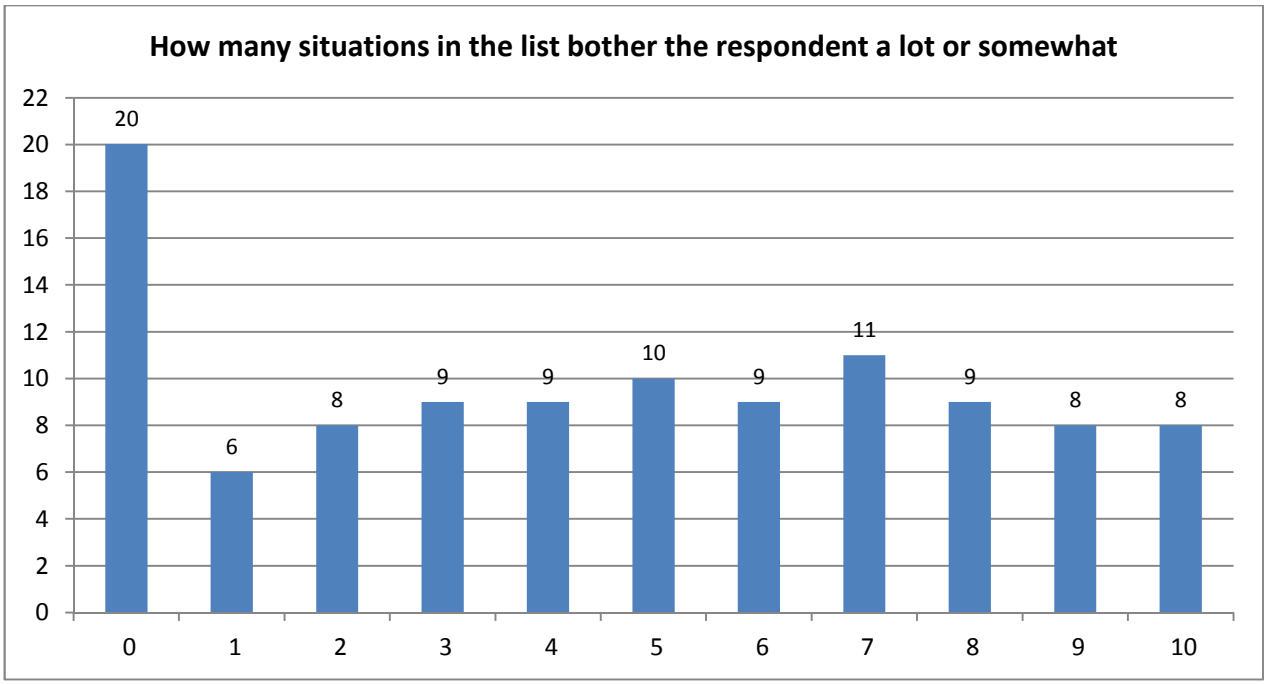

Figure 20: Summarised list of different situations that bother people (% of Internet users, n=799)

In case of the question that was answered by all the respondents, two of the three most disturbing situations involved children – the kindergarten shows pictures of a child on its web page (bothered 44%) and a teacher follows the students' activities on Facebook (bothered 38%) (Figure 21). The latter situation especially bothers those who are pupils or students themselves (bothered 69%). On the other hand, security cameras in schools disturbed only 17% of the respondents (the percentage was once again considerably higher among pupils and students – 35). Many of the respondents were not bothered by police surveillance cameras in the city space (bothered only 13%).

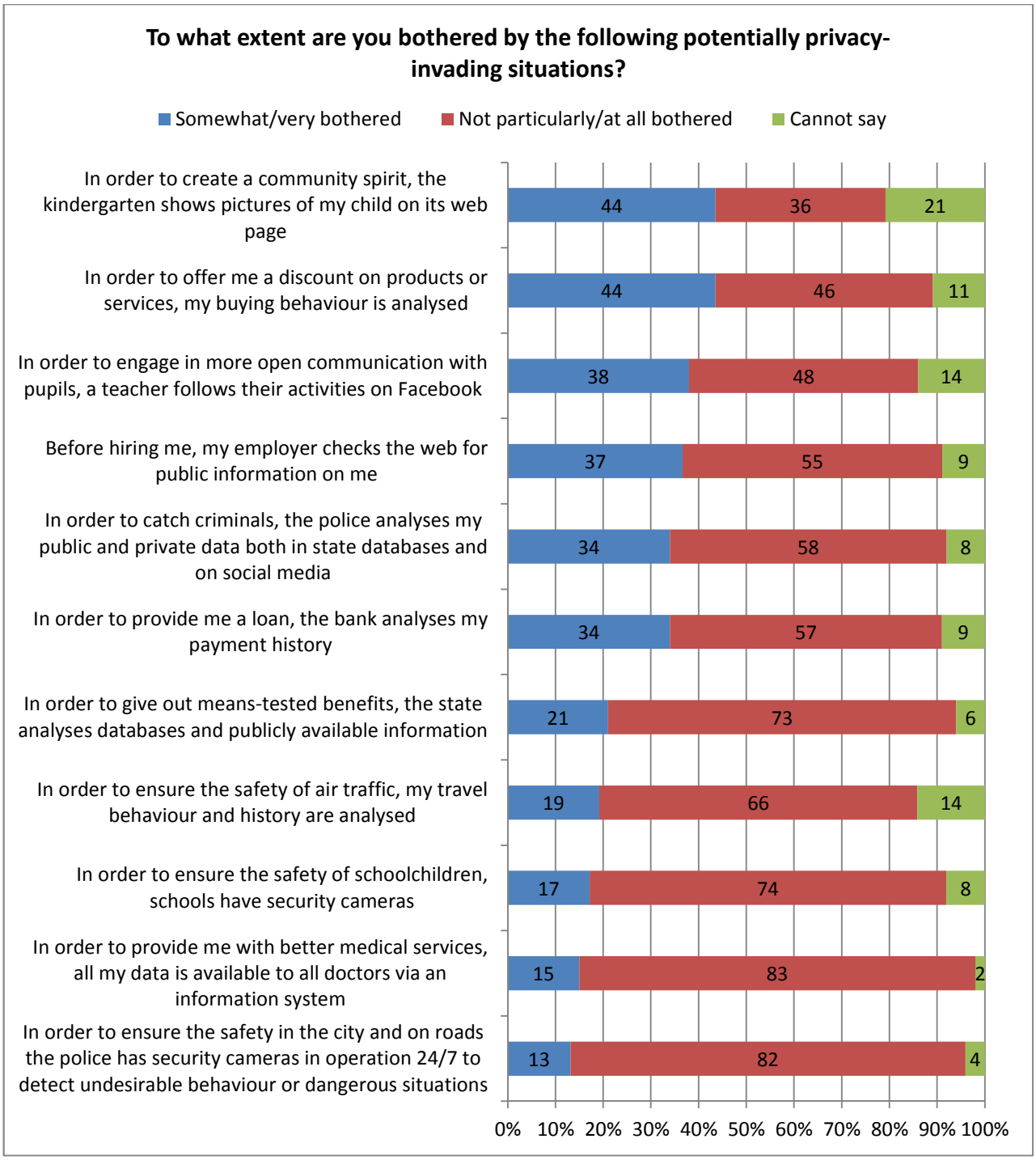

Figure 21: How much people are bothered about different sample situations (% of all respondents, n=959)

In case of the question answered only by the Internet users, the most disturbing situations were the ones in which a service provider asked and analysed a user's data and behaviour (a mail service provider analyses the content of e-mails – bothered 65%; apps in mobile and online environments use personal data – bothered 54%), or which were related to social relationships (friends publish party pictures on the Internet – bothered 60%; data of a child is published in Perekool forum – bothered 51%). The respondents were the least bothered by situations of personal gain, for instance sharing their location data to get restaurant, parking or taxi recommendations (bothered 31%), and by publishing workout data to get recommendations and gain well-wishers (bothered 39%) (Figure 22).

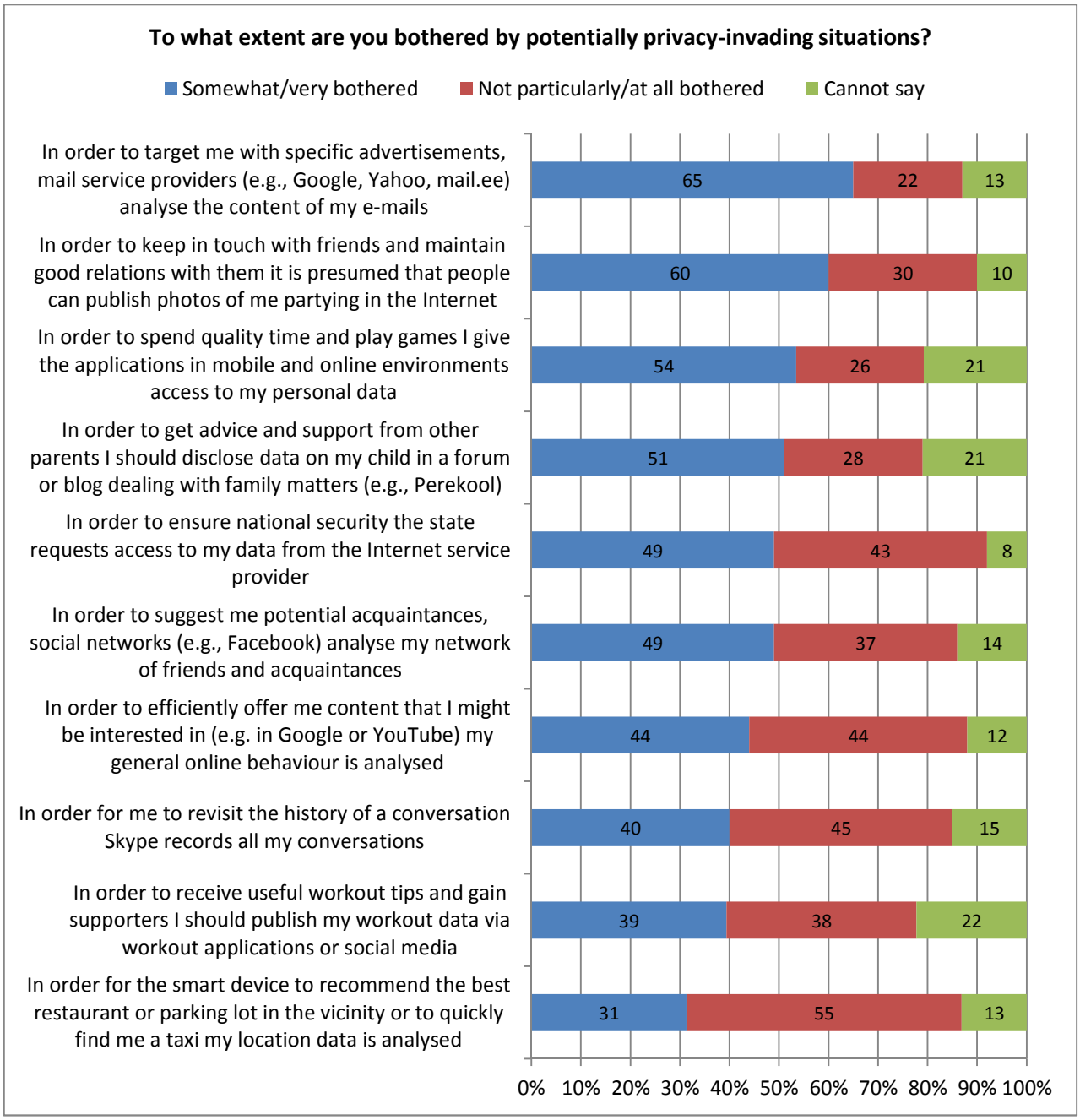

Figure 22: How much Internet users are bothered about different sample situations (% of Internet users, n=799)

Situations concerning children are a bit more disturbing for women: 47% of them are bothered if a kindergarten displays pictures of the child on its webpage, whereas it disturbs 40% of men; pressure about disclosing data on one's child in some family forum or blog (e.g., Perekool) is disturbing for 56% of women and 47% of men.

It is worth mentioning that more than half of the respondents (55%) agreed to the claim that "If possible I use my Facebook or Google account to log into various environments"; as was to be expected, younger people use this possibility more than older age groups (75% of young people versus 55% on average). Even if people do not trust Internet companies, the trade-off is usually sufficient to still use the service.

WHO SHOULD PROTECT PEOPLE'S RIGHT TO PRIVACY?

When we analyse the issue of personal data, including the question of who should protect it and be responsible for or react to the violation of privacy, we cannot look past the complexity of the topic and the need to consider different contexts. It is nearly impossible to phrase universal solutions and often a decision can only be made on a case-by-case basis.

Most frequently people thought that the responsibility for personal data on the Internet fell on the individual person (84%), similar results were also received in the Eurobarometer on privacy (Special Eurobarometer 359... 2011). The state was seen as responsible in 24% of the cases in this study, while the European Union's responsibility was claimed by a considerably larger percentage – 55% (Figure 23). Placing responsibility on the European Union institutions could be directly linked to media coverage of, for instance, the ruling of the European Court of Justice, according to which people can from now on demand from search engines to have incorrect personal data erased. People could expect that national and international structures lay down regulations to protect them and set limits to third parties. Public discussions have also covered the long process of renewal of the data protection legislation of the European Union.

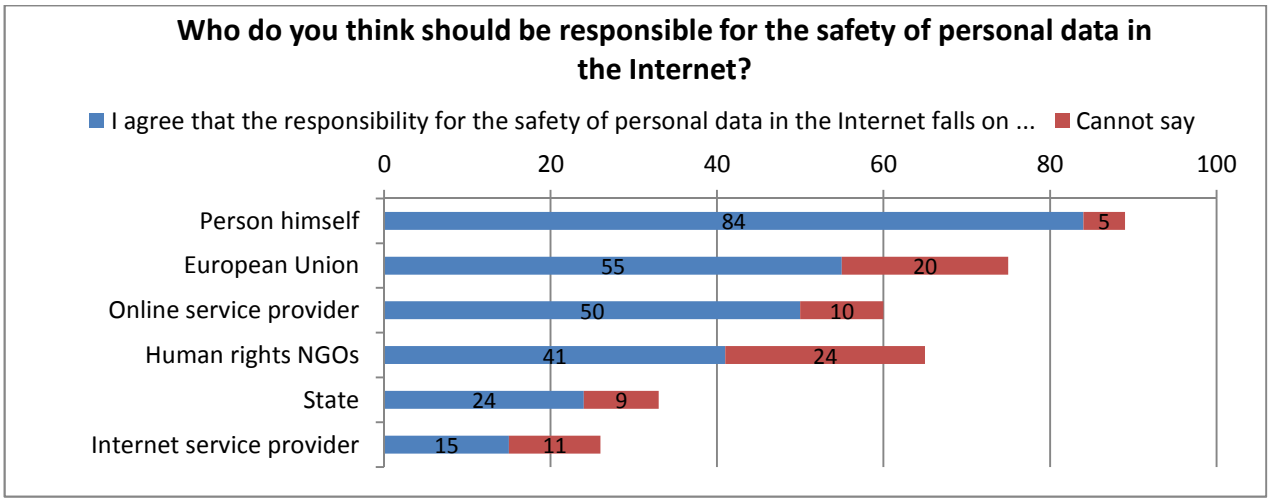

Figure 23: Who the respondents think should be responsible for the protection (in the sense of limitations) of personal data on the Internet (% of all respondents, n=959)

Merili Oja, advisor in the Ministry of Justice: *"Laws cannot be made stricter; laws can be made better. When drafting regulations, we need to find a balance between the protection of private data and other basic rights, such as the freedom of enterprise and security. I agree that data processing by the state needs to be more regulated, especially in relation to the notification of the data subject."*

Even though people do not mostly think that the state is responsible for the protection of personal data, there are several ways in which the state can play a role. We asked our experts what the state could do to defend people's right to privacy.

Experts largely agreed that legislation should provide a general framework but overall responsibility should not be taken away from people, as this would lull them into false security and place the responsibility away from them.

Therefore, on the basis of survey results and expert interviews, we can see that personal responsibility comes foremost. People can apply their responsibility in various ways, such as by being aware of the conditions of use of different services. 47% of respondents claimed that they always or most of the time read the privacy policy and conditions of use of a service, 22% do it sometimes and 22% do it seldom or never (Figure 24).

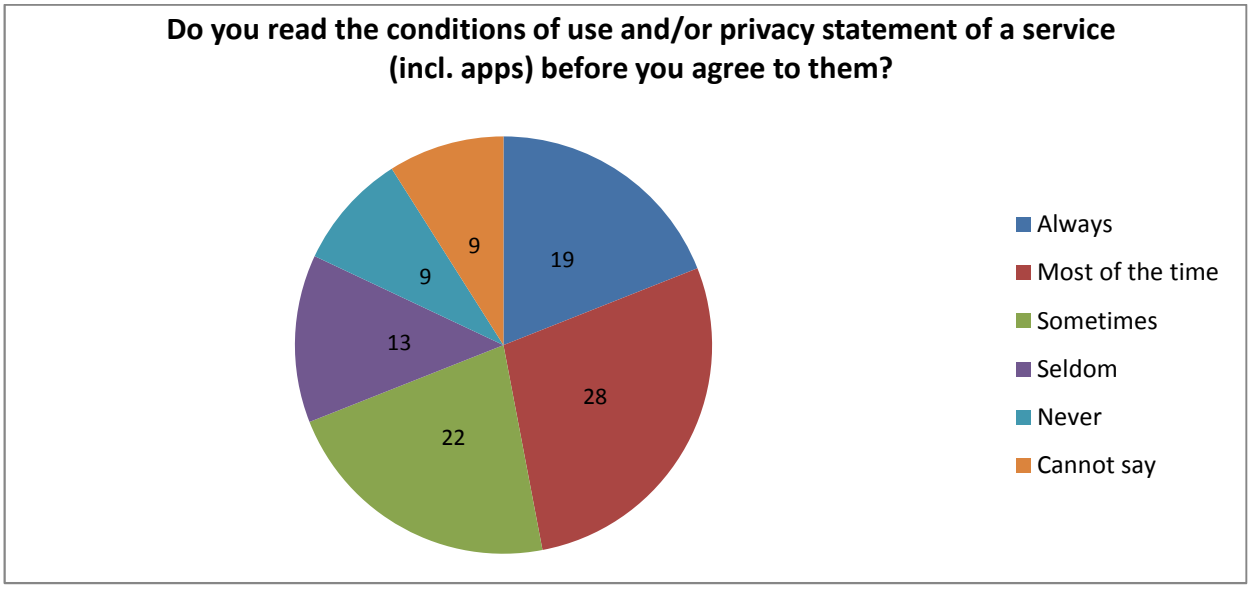

Figure 24: To what extent do people read the privacy statement (% of all respondents, n=959)

A noticeably large share of respondents say that they always or mostly read the privacy statement and/or conditions of use. From the point of view of raising people's awareness, this is certainly a positive outcome, but we should point out that in this case we might be dealing with socially recommendable answers (i.e., people reply the way they "are expected to"). We also should not forget that people's ideas of "reading" the conditions might differ – it could just mean that an app is given permission to access data, just the first sections are scanned over, a thorough analysis with the help of a dictionary is carried out and so on. Since we asked this question from everyone, it can be assumed that some of the respondents had paper contracts in mind, which have nothing to do with online services. Somewhat surprisingly, we did not notice large differences between active and moderate Internet users, whereas the non-users did stand out (Figure 25).

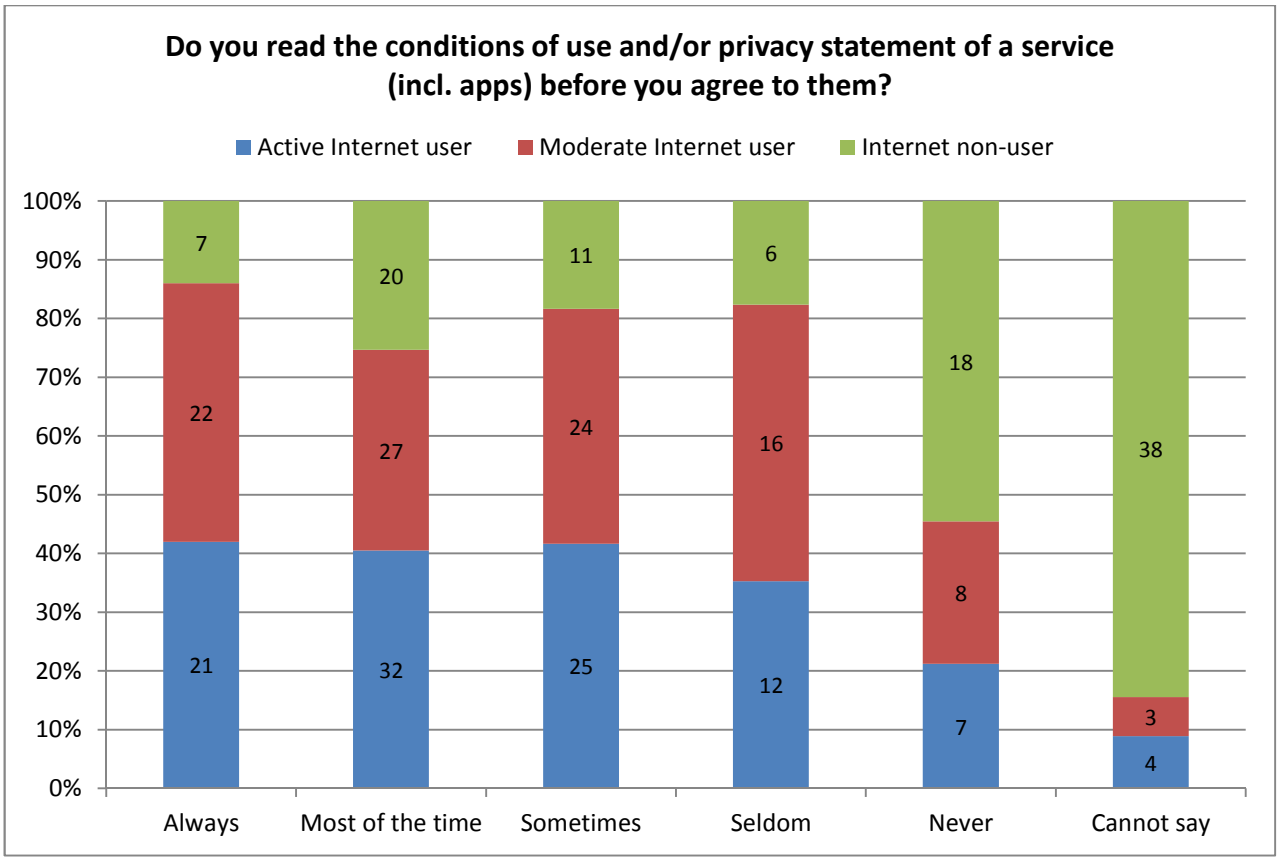

Figure 25: Comparison of people grouped by the frequency of the Internet use in regard to reading conditions of use and privacy statements (% of respondents, n=959)

Expert focus groups brought out that the online conditions of use and privacy statements are very long as a rule and that even people who deal with the right to privacy daily do not manage to read them in reality.

Age-wise, we can see (Figure 26) that the options "always" and "most of the time" have some differences; although all age groups have a roughly equivalent share of both answers (42-51%), the percentages stay similar as the age of the respondents grows. What we can see in case of older respondents is that the amount of those who cannot answer the question suddenly increases (2% vs 24%); this could partially indicate the insufficiency of digital literacy but is also linked to general Internet use (63% of 65-74-year-olds use the Internet).

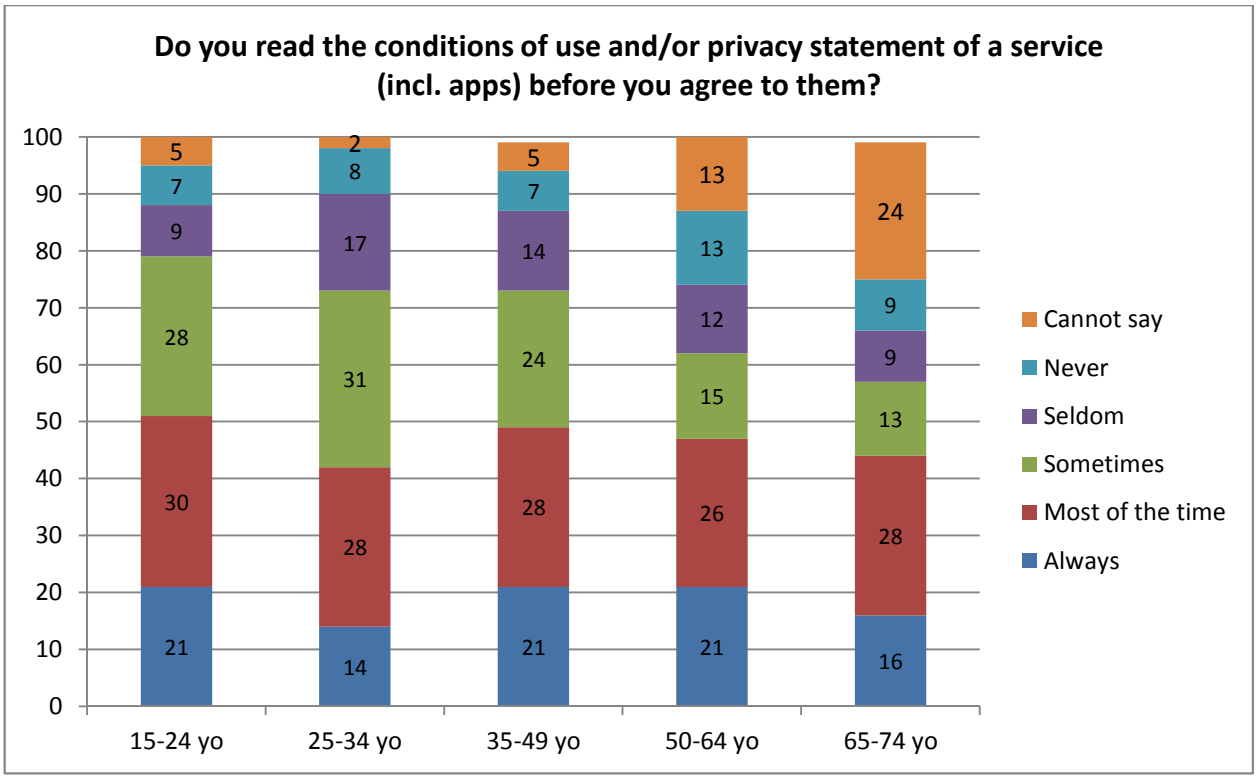

Figure 26: To what extent do people read the privacy statement, comparison by age (% of all respondents, n=959)

Technology journalist Hans Lõugas:
"There is a strong social expectation to read these conditions. Would it be possible to somehow enforce a rule that these awfully long privacy statements be made shorter in the interest of legal clarity?"

With the privacy statements and conditions of use, we could ask how informed is "the informed consent" in reality – if the description of conditions of use is complicated and long and it is very easy for people not to have to make a decision ("to use click on a button and you have agreed"), then this cannot really be considered informed consent.

Next, we wanted to know the following three aspects in relation to the opinions about the protection of privacy – to what extent have people sensed that their privacy had been violated; where would they hypothetically turn if they sensed a violation; and where have they really turned to in order to have their privacy protected. Here, we would like to remind readers that we did not examine objective invasions of privacy, i.e. how the respondents should have acted according to law, but when and how people perceive violations and what they have done or say that they have done to protect their privacy.

Figure 27 shows that the biggest share of people, 16%, have sensed that their privacy has been violated by strangers, while 15% named Internet service providers as perceived violators. 11% claim that their privacy has been violated by private enterprises within the past year, and the same number was true in the case of friends and close ones.

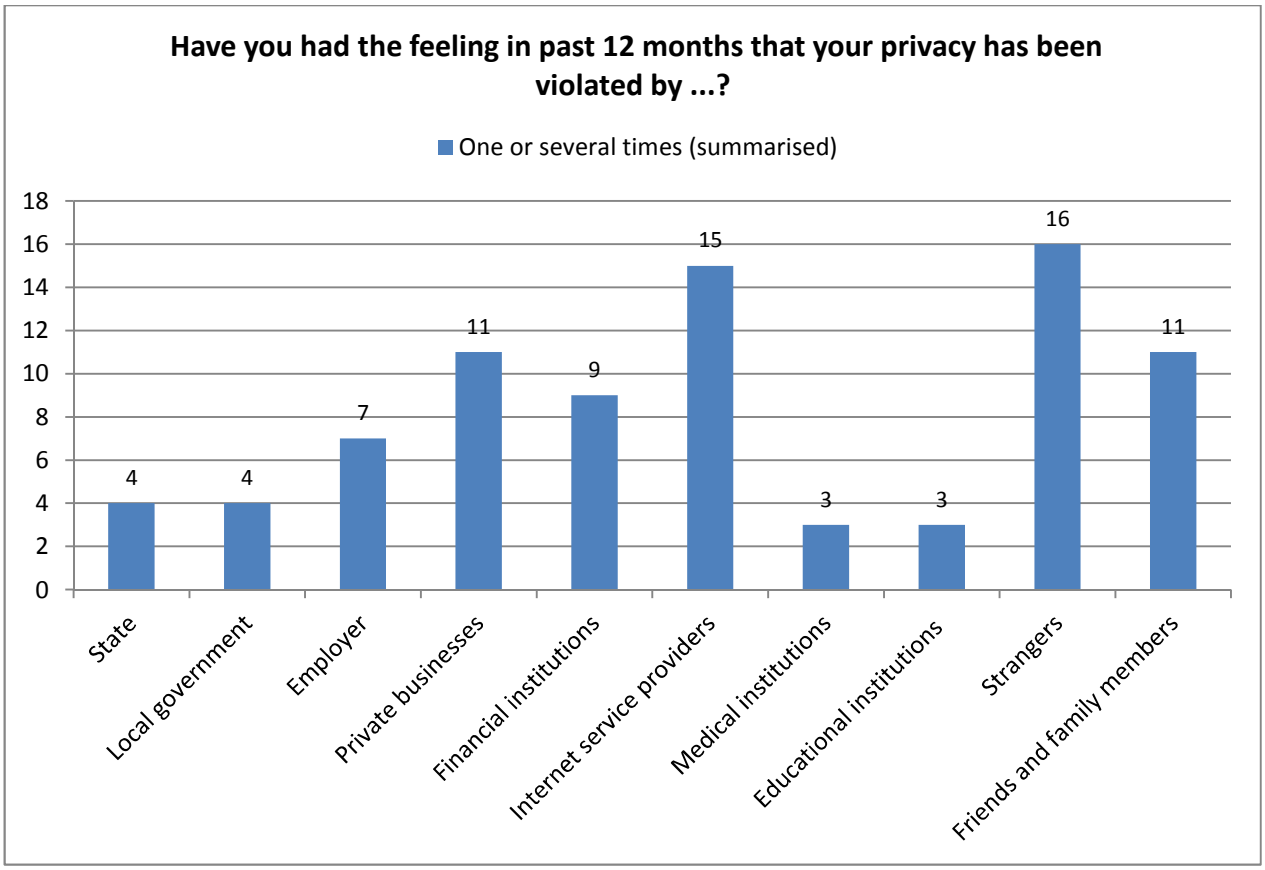

Figure 27: Perceptions of privacy invasions by respondents (% of all respondents, n=959)

Where would people turn in order to protect their privacy in web environment? The questionnaire listed different persons, offices and institutions to whom people could potentially turn. Some of the offered options included institutions or authorities that could be related to and deal with the issue of privacy from some angle, but that do not process complaints and requests related to the violation of the right to privacy. Therefore, it would not make sense to turn to such institutions as the Information System Authority, Consumer Protection Board, Ministry of Justice and so on.

Katrin Merike Nyman-Metcalf, head of the Chair of Law and Technology of Tallinn University of Technology: *"The Data Protection Inspectorate has a very important role to fulfil in this matter. Their decisions should be easily accessible as this would help people understand what has gone wrong. They shouldn't focus on punishment, but on informing. Ordinary citizens should have the possibility to read clearly phrased decisions."*

As was expected, the respondents said that privacy violations should primarily be handled by the Data Protection Inspectorate (77% of respondents would consider turning to the Inspectorate to protect their rights), the main task of which is supervision in relation to data protection (Figure 28). The same amount of people (also 77%) mentioned the police. Many of the respondents (73%) thought that the person or organisation that invaded the privacy should deal with the violation. 68% would hypothetically turn to the Consumer Protection Board, 55% to the court and 53% to the Information System Authority.

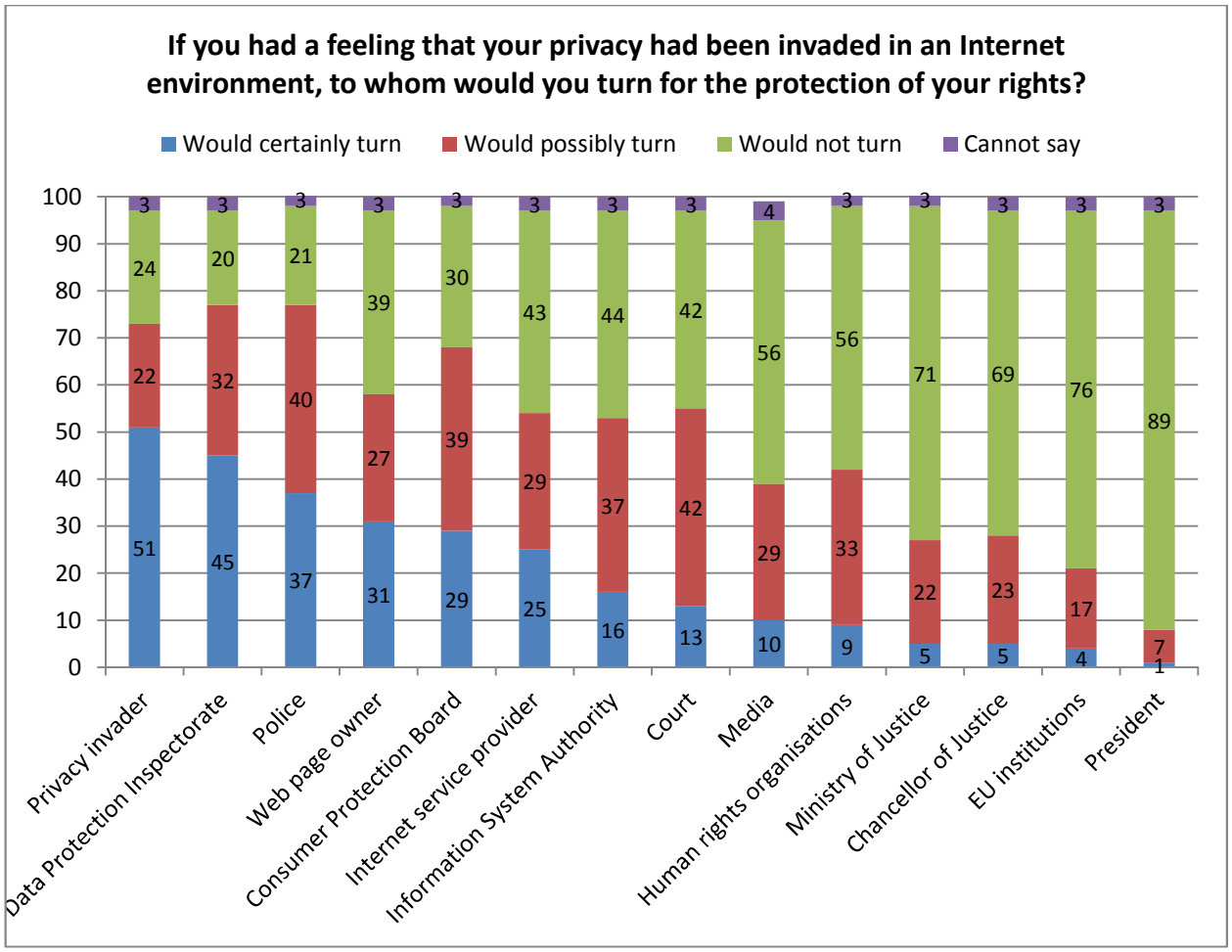

Figure 28: Where would people turn for the protection of privacy-related rights (% of all respondents, n=959)

The least number of people would turn to the President (8%), the European Union institutions (21%), the Ministry of Justice (27%) or the Chancellor of Justice (28%). In relation to the European Union, we would like to remind readers that in one of the previous questions (Figure 23) people considered the EU to be responsible for data protection. Katrin Merike Nyman-Metcalf, head of the Chair of Law and Technology of Tallinn University of Technology, stressed in the expert focus group that people could sense the pressure to give the "right" answer: "For instance, that they would turn to the EU for the protection of their rights. People think that they should and that's why they give this answer, even if they do not really think that the EU could really do anything."

Technology journalist Hans Lõugas:
"The media plays an important role – it has to unite expert knowledge, people's needs and policymakers."

40% of respondents said that they would turn to the media if necessary. The role of the media as a watchdog in society is also important in relation to privacy protection, but we should keep in mind that the coverage of delicate incidents with the help of the media draws a lot of attention to the matter and defies the purpose of the whole matter.

When we asked the respondents how many times they had turned to someone to protect their privacy, 5% (46 people) replied that they had contacted various persons, authorities and institutions to defend their rights. The most common answers were that they had turned to the website owner (20 people) or to the person/organisation that invaded their privacy (20 people); on several occasions, people said that they had contacted the police (13 people)

and the Internet service provider (11 people). In some cases, people had turned to the Consumer Protection Board (8 people) and to the Data Protection Inspectorate (7 people).

In most of these cases, the Data Protection Inspectorate would probably be the best choice among the institutions to ask for help, but survey results do not reflect this in people's preferences. Hence, we can assume that people are uncertain as to where they should turn, so we might be dealing with insufficient information.

> ***Silver Sarapuu, advisor in the Data Protection Inspectorate:*** *"Society can be divided in two: older people who know what to do to protect their privacy, but who do not care, because nothing has ever happened and never likely will. And then young people whose awareness we need to address from early on. If your privacy has not been taken away from you for a little while, nothing changes. The new generation could be taught to think more."*

Experts in the focus group mentioned the general need to raise awareness from several aspects: first, people should notice the problem (the role of media); second, people should have easy access to relevant and understandable information (e.g. sample cases from the Data Protection Inspectorate); third, digital literacy should be handled systematically and diversely, starting with elementary education (good example is Information System Authority's net sheep cartoons); fourth, the state should inform its citizens more efficiently about when, what and why information is collected and processed about them.

HOW WOULD IT BE POSSIBLE TO PROTECT PEOPLE'S PRIVACY?

There are a number of different technology-based strategies to protect privacy; we listed some of the more common ones to the respondents in our survey (a total of 19 activities). We only asked this question from Internet users. As a rule, people chose several options for protecting their privacy, and 10-12 activities from the list were used the most (Figure 29).

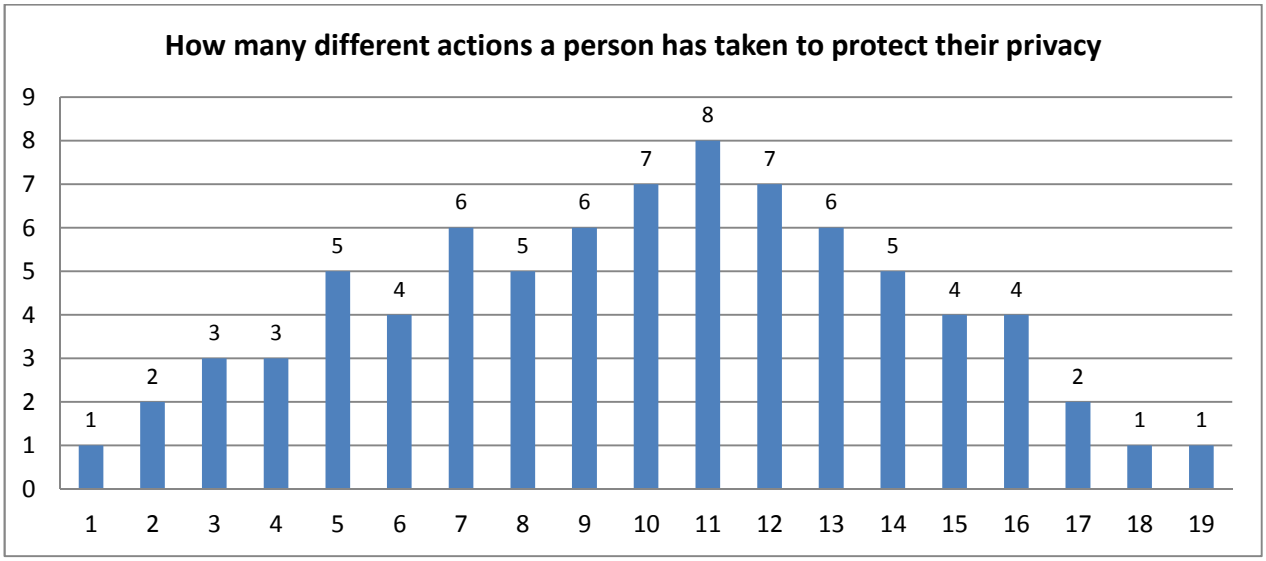

Figure 29: Summarised list of different activities a person has done to protect his or her privacy (% of Internet users, n=765)

As already mentioned, many different activities and strategies can be used to protect online privacy, which could, in general, be divided into four categories (without the intent to achieve balance in covering all these types):

Preventive social strategies related to content creation and consumption (marked with PS on the Figure), which means self-censoring and limiting content creation and usage frequency:

- Has refrained from sharing information on the Internet
- Has only shared information on the Internet to a small extent
- Has shared information in a way that it is understandable to only a few select people
- Has refrained from opening an account in a web environment
- Has refrained from downloading an application
- Has restricted the number of people who can access the information
- Has used several identities on the Internet (e.g. pseudonyms, false names)
- Has published false data about oneself on the Internet

Preventive technical strategies (marked with PT on the Figure), which are related to taking and applying preventive technical measures:

- Has avoided the use of public Wi-Fi networks
- Has used privacy settings offered by a web environment or application
- Has used the screen lock function of a phone, computer passwords, fingerprint readers, login with ID card, mobile ID
- Has used the possibility to encrypt documents or messages
- Has used security software (e.g. anti-virus software, security settings of an operation system)
- Has refrained from buying from an online store that does not have a security certificate, a secure online store sign or some other measure/tool to ensure safe shopping
- Has used different passwords in different environments

Reactive strategies related to content creation and consumption (marked with RS on the Figure); options applied after the sending of information:

- Has deleted information about oneself on the Internet
- Have asked others to delete information about him or her on the Internet
- Has deleted an account from a web environment

Reactive technical strategies (marked with RT on the Figure); this primarily signifies ways in which people take measures after the information has been published:

- Has cleared the browser history or deleted cookies

The questionnaire results show that the most popular strategy is the limited sharing of information, followed by more technical strategies, such as security software, screen locks and passwords (Figure 30).

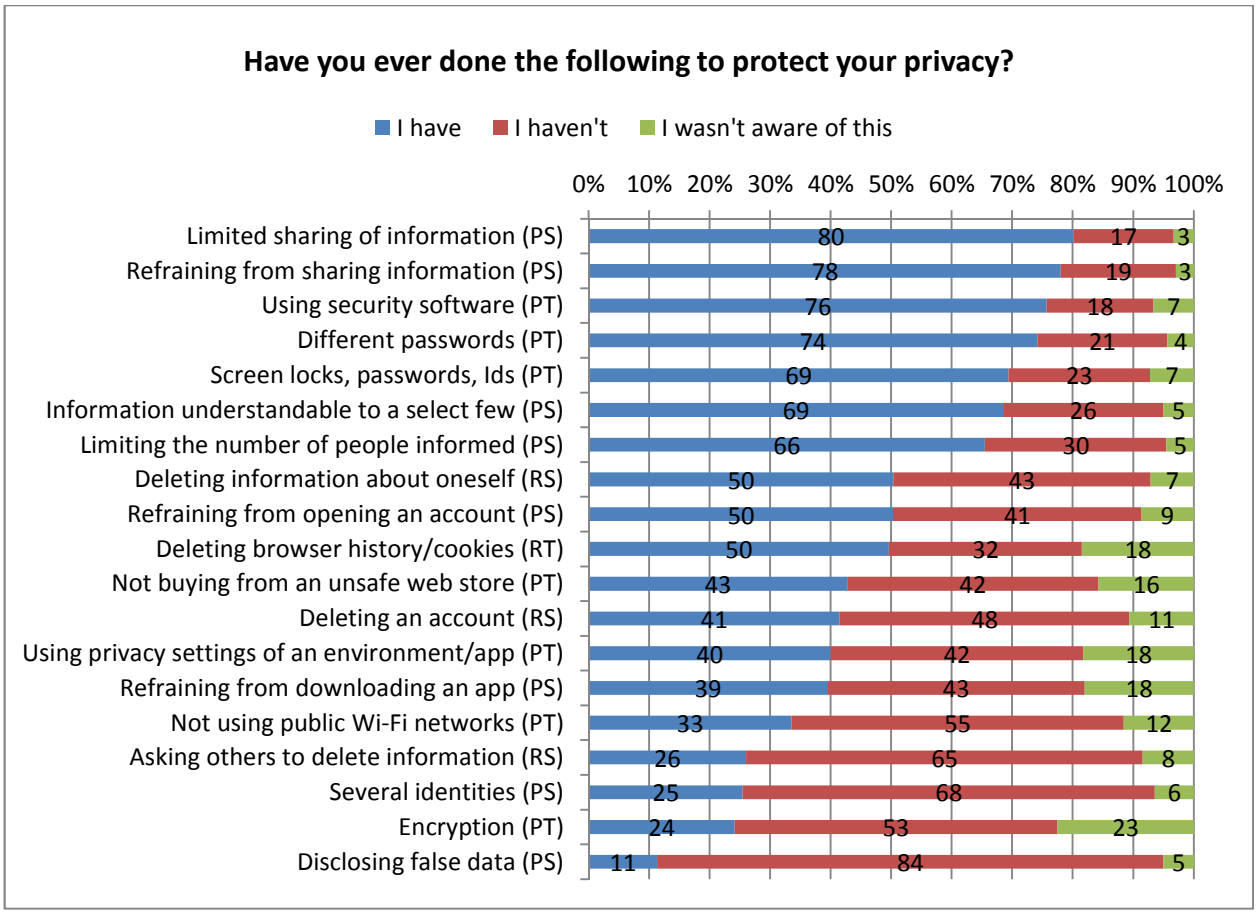

Figure 30: Possible privacy-protecting activities in order of popularity (% of Internet users, n=799)

Of social strategies, 69% of respondents have used social steganography, i.e. they have shared information so that it was understandable to only a certain part of the audience (boyd 2010a). There are many different social strategies, including some really complicated ones like whitewalling and super-logoff (boyd 2010b).

The least used strategies were presenting false information about oneself (11%) (a similar activity, mentioned only by 25%, is using multiple identities) and document encryption (24%).

Third sector activist Siim Tuisk: *"Strategies are complicated. For instance, some people delete their Facebook account every time they have finished using it for that time. This way, the account stays invisible, in the deletion queue. However, this action can be reversed and the account can be reactivated with all the friends and other information. This is done so that Facebook could not use these people's data and that no one could look them up."*

A tell-tale result is that people responded by saying they were not aware of certain strategies – the least amount of people know about the possibility to encrypt documents and messages (23% do not know); the next answers, with 18% being unaware, were the following options (full wording noted here) "I have cleared the browser history or deleted cookies", "I have used privacy settings offered by a web environment or application" and "I have refrained from downloading an application". 16% were not aware of the possibility to refrain from "buying from an online store that does not have a security certificate, a secure online store sign or some other measure/tool to ensure safe shopping". We can see that in all the

mentioned options we are dealing with somewhat complicated technological terminology (encryption, browser, cookies, app, certificate), which are presumably not part of people's digital literacy vocabulary.

The results of the question about activities done to ensure privacy are similar to the findings of the 2011 Eurobarometer (Special Eurobarometer 359... 2011), which showed that Europeans mostly used limited information sharing strategies, technical and procedural strategies. When comparing the results of the two studies, it becomes evident that (covered in both surveys) usage activity has risen in the case of comparable activities (obviously taking into account the different contexts of the studies) – in 2011, 36% of respondents claimed to use antivirus programmes; now it's 76%. Cookies had been deleted by 29%; now it's 50%. The security elements of a web page had been checked by 27%; these days 43% do it.

Answers given by men and women were rather similar in this study, though some differences were notable in the following privacy-protecting activities (women tend to use more social strategies, while men prefer technical strategies) (Figure 31):

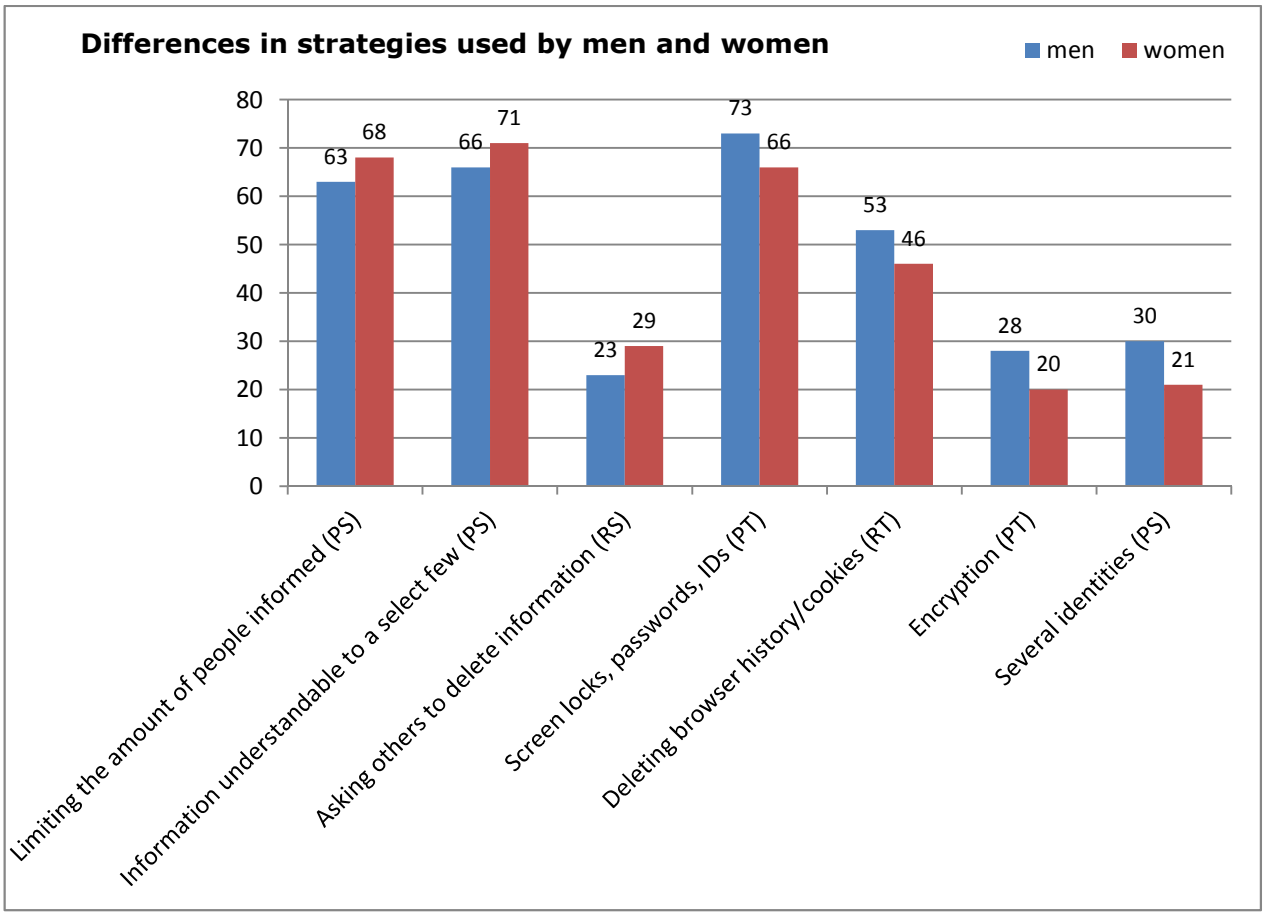

Figure 31: Men vs. women in potential privacy-protecting activities (% of Internet users, n=799)

Figure 32 summarises the average amount of privacy-protecting actions in different groups by sociodemographic indicators. We can see notable differences by age, nationality and education, while gender does not play a role in this case, unlike in the previous point of analysis. Younger people clearly have a wider repertoire of possible protective activities and the variety decreases significantly as the age rises. In an pan-European study, EU Kids Online, it was discovered that Estonian youngsters belong to the "high use – high risk" category – almost all youngsters use the Internet and their behaviour is riskier in comparison to the European average (Kalmus 2012). Here, we should also note that the selection of protective activities is wider in relation to the people whose general behavioural patterns on

the Internet could put them in more danger. People who use the Internet for limited activities (e.g., just to read newspapers) do not sense the threats and in turn the need to apply different strategies.

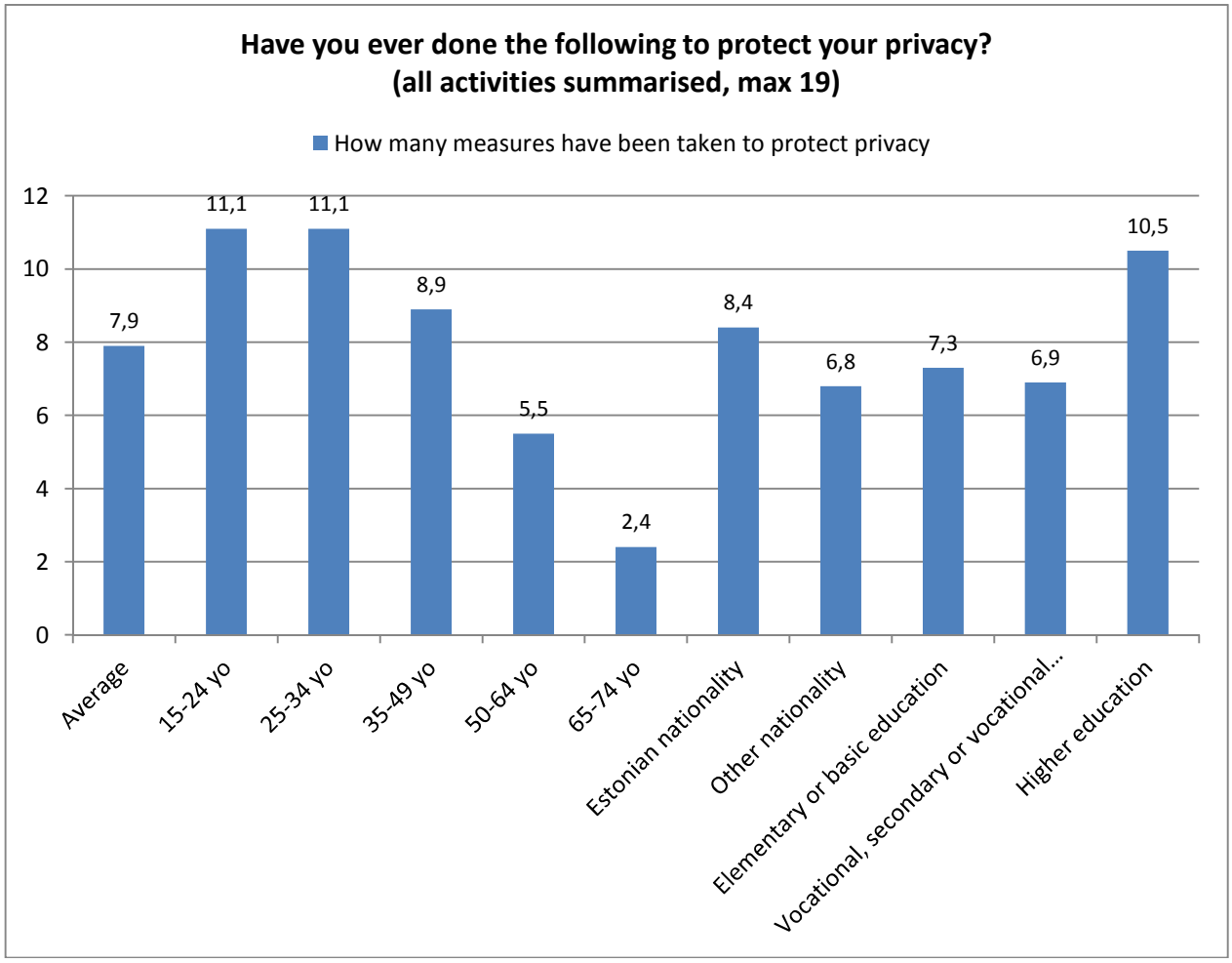

Figure 32: Average of the summarised list of different measures that a person has taken to protect his or her privacy by sociodemographic factors (average in a given group, n=799)

Additionally, we compared the amount of privacy-protecting measures in terms of active and moderate Internet users, taking into account only those strategies that showed statistically significant differences (Table 3). We can see that the biggest difference is evident in the case of the respondents who said that they had not been aware of such a possibility – it does not come as a surprise that active Internet users are more familiar with different strategies and take privacy-protecting measures more often than moderate Internet users. In the case of active Internet users, the average number of activities is 10.4 and in case of moderate users it is two less on average – 8.4.

Table 3: Active vs. moderate Internet users by the amount of privacy-protecting measures used (% of Internet users, n=799)

	Active Internet user – has taken this measure	Moderate Internet user – has taken this measure	Active Internet user – is not aware of this possibility	Moderate Internet user – is not aware of this possibility
Has shared information only to a limited extent	85%	75%	2%	5%
Has used security software (PT)	83%	68%	3%	11%
Different passwords (PT)	81%	67%	2%	7%
Screen locks, passwords, IDs (PT)	73%	65%	4%	11%
Information that is understandable only to a few select people (PS)	74%	63%	9%	2%
Has limited the number of people who receive the information (PS)	76%	55%	2%	7%
Has deleted information him- or herself (RS)	57%	44%	5%	9%
Has deleted browser history/cookies (RT)	60%	38%	11%	27%
Has deleted an account (RS)	50%	33%	8%	13%
Has used the privacy settings of an environment/app (PR)	52%	27%	11%	26%
Has refrained from downloading an app (PS)	45%	34%	11%	26%
Does not use public Wi-Fi networks (PT)	30%	38%	7%	17%
Several identities (PS)	33%	17%	5%	8%
Encryption (PR)	28%	20%	18%	27%
Disclosing false data (PS)	16%	7%	4%	6%

Many strategies, presumably, just never enter the moderate user's mind – for instance, if one only uses the Internet for online banking, the idea of disclosing false data is unthinkable. Most commonly, the answer of "I was not aware of this possibility" was given as a reply to the question about data encryption (27% of moderate users and 18% of active users), to the question about deleting browser history and cookies (27% of moderate users, 11% of active users) and to strategies related to applications (26% of moderate users, 11% of active users). Once again, it could be noted that these options contain rather specific terminology.

In relation to differences: the usage frequency of strategies varies between active and moderate user groups within an 8-25% range. The statistically significant difference in responses is the least notable in terms of the encryption strategy – the usage frequency is low in both instances, the difference being 8%; the largest gap emerges in relation to the strategy where the privacy settings of web environments and apps are adapted – moderate users apply this strategy 25% less than active users. A surprising result was the use of public Wi-Fi networks – this was the only strategy that the moderate users applied more than the active users (38% of moderate Internet users and 30% of active users claimed to have applied this strategy).

To conclude the study results chapter, we would like to repeat that the objective of the study was not to evaluate what is right and wrong or to map actual violations; our attempt was rather to understand how people interpret the right to privacy in general and what kind of tendencies become apparent from the opinions expressed in the questionnaire. Conclusions and policy recommendations are presented in the following chapters of the study.

REFERENCES

1. Albrechtslund, A. (2008). Online Social Networking as Participatory Surveillance. *First Monday*, 13(3). URL: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2142/1949
2. Andrews, D. (2003). Electronic Survey Methodology: A Case Study in Reaching Hard-to-Involve Internet Users. *International Journal of Human–Computer Interaction*, 16(2), 185–210.
3. Bax, S. (2003). CALL-Past, Present and Future. *System*, 31, 13–28.
4. boyd, d. m. (2007). Social Network Sites: Public, Private, or What? *Knowledge Tree,* 13. URL: http://www.zephoria.org/thoughts/archives/2007/05/07/social_network-3.html
5. boyd, d. m. (2010a). Social Steganography: Learning to Hide in Plain Sight. *danah boyd's blog*, 23 August. URL: http://www.zephoria.org/thoughts/archives/2010/08/23/social-steganography-learning-to-hide-in-plain-sight.html
6. boyd, d. m. (2010b). Risk Reduction Strategies on Facebook. *danah boyd's blog*, 8 November. URL: http://www.zephoria.org/thoughts/archives/2010/11/08/risk-reduction-strategies-on-facebook.html
7. Eurostat news release. Internet access and use in 2012. (2012, 18 December). URL: http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-18122012-AP/EN/4-18122012-AP-EN.PDF
8. Infotehnoloogia leibkonnas: IT32: 16-74-aastased arvuti ja Interneti kasutajad isikute rühma järgi. (2014). *Database of the Estonian Statistics Office*.
9. Infotehnoloogia leibkonnas: IT38: 16-74-aastased Interneti kasutajad elukoha ja kasutuseesmärgi järgi. (2014). *Database of the Estonian Statistics Office*.
10. Kalmus, V. (2013). Laste turvalisus uues meediakeskkonnas. In the book: M. Heidmets (ed.), *Eesti inimarengu aruanne 2012/2013: Eesti maailmas*. Tallinn: Eesti Koostöö Kogu. Pp. 83–85. URL: http://www.kogu.ee/wp-content/uploads/2013/05/EIA20122013.pdf
11. Kalmus, V., Keller, M. & Pruulmann-Vengerfeldt, P. (2009). Elukvaliteet tarbimis- ja infoühiskonnas. In the book: M. Lauristin (ed.). *Eesti Inimarengu Aruanne 2008.* Tallinn: Eesti Ekspressi Kirjastus. Pp. 102–124. URL: http://kogu.ee/public/EIA08_est.pdf
12. Larsen, M. C. (2007). 35 Perspectives on Online Social Networking. *Social Computing Magazine*, 5 July. URL: http://vbn.aau.dk/files/17515817/35_Perspectives_on_Online_Social_Networking_by_Malene_Charlotte_Larsen.pdf
13. Livingstone, S. & L. Haddon. (2009). *EU Kids Online: Final Report*. LSE, London: EU Kids Online. URL: http://www.lse.ac.uk/media@lse/research/eukidsonline/eu%20kids%20i%20(2006-9)/eu%20kids%20online%20i%20reports/eukidsonlinefinalreport.pdf
14. Marwick, A. E., Murgia-Diaz, D. & Palfrey, J. G. (2010). Youth, Privacy and Reputation (Literature Review). *Berkman Center Research Publication No. 2010-5; Harvard Public Law Working Paper No. 10-29*. URL: http://ssrn.com/abstract=1588163

15. Miles, S. (2003). Young People in a Globalizing World. In the book: *World Youth Report 2003*. New York: United Nations. Pp. 290-303.
16. Pruulmann-Vengerfeldt, P. (2006). *Information technology users and uses within the different layers of the information environment in Estonia*. (Dissertation, Tartu University) Tartu: Tartu University Press.
17. 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. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1928498
18. Solove, D. J. (2007). 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review,* 44, pp. 745–772. URL: http://ssrn.com/abstract=998565
19. Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union. (2011). *European Commission*. URL: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

ANNEXES

Annex 1 – questionnaire