The Internet & Surveillance - Research Paper Series

Edited by the Unified Theory of Information Research Group,
Vienna, Austria (http://www.uti.at)

ISSN 2219-603X

Title: Research Design & Data Analysis, Presentation, and Interpretation: Part Two

Author: Verena Kreilinger

Research Paper Number #14

Date of Publication: April 2014

Author Institution: Unified Theory of Information Research Group

Author Address: Steinbrechergasse 15, 1220 Vienna, Austria

Author e-Mail: verena.kreilinger@uti.at

Author URL: www. sns3.uti.at

Acknowledgement: The research presented in this paper was conducted in the project "Social Networking Sites in the Surveillance Society" (http://www.sns3.uti.at), funded by the Austrian Science Fund (FWF): project number P 22445-G17. Project co-ordination: Dr. Christian Fuchs

Research Design & Data Analysis, Presentation, and Interpretation: Part Two

Verena Kreilinger

Keywords: Research Design, Usage of Social Networking Sites, Privacy Concern Index, Surveillance Knowledge Index, Surveillance Critique Index, Carefulness of Information Behaviour, Usage Intensity, Field of Study, Targeted Advertising on Social Networking Sites

Short biography of the author: Verena is a postgraduate student at the University of Salzburg, majoring in communication studies. She currently is a research associate in the project "Social Networking Sites in the Surveillance Society". Verena graduated from the University of Applied Sciences Salzburg with a master's degree in Digital Media Studies in 2007. Prior to joining the Unified Theory of Information Research Group, she worked in advertising and production. Verena is member of the editorial team of "tripleC: Journal for a Global Sustainable Information Society" and participant in the European Cooperation in Science and Technology Action "Living in Surveillance Societies"- Working Group 3 "The Business of Surveillance".

Table of Content

List of Figures

List of Tables

For successfully conducting social research a well-defined research design is decisive. It serves as a blueprint for the study, clarifies the purpose of the study, as well as links research question to the respective research methods. Based on Babbie (2010, 114) and Punch (2005, 63), a research plan contains the following elements:

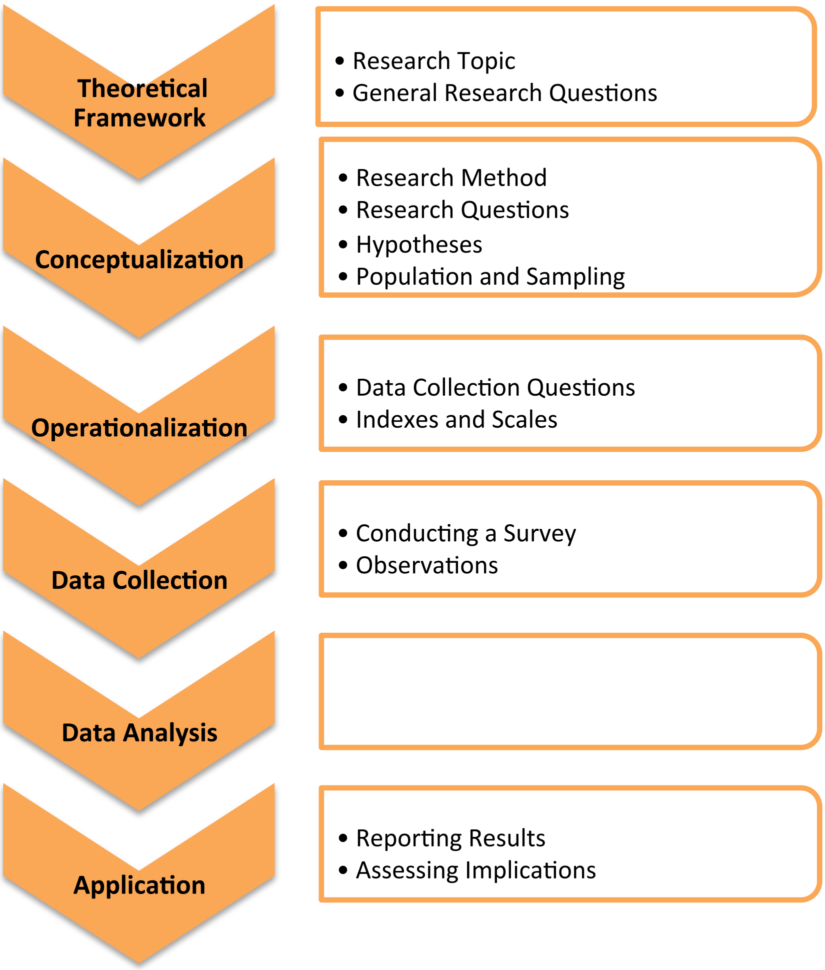


Figure 1: Elements of a Research Design

As figure 1 illustrates, the first step is to outline and examine the overall research topic, by asking general research questions, assembling ideas and theoretically assessing the research area. The second step is to specify the research questions, and - if suitable – to develop some hypotheses. By conceptualizing the research, all relevant concepts and variables need to be specified, the best-suited research method is chosen and population and sampling are defined. The next step is to operationalize the concepts, by developing data collection questions and setting up scales and indexes. Fourth, the data is collected – by conducting a survey, an experiment, field research or any other kind of method. In the fifth step, the data is processed and analyzed in order to finally draw conclusions, answer research questions, and assess implications (Babbie 2010, 283–287; Wright 2005; Couper 2001; Kaplowitz, Hadlock, and Levine 2004; Ilieva, Baron, and Healey 2002; Evans and Mathur 2005; Lefever, Dal, and Matthíasdóttir 2007; Yun and Trumbo 2000).

1. Theoretical Framework

Punch stresses the importance of data and theory, which he calls "the two essential parts to science" (Punch 2005, 8). Babbie similarly highlights that "the two pillars of science are logic and observation" (Babbie 2010, 10). According to Punch "the objective of scientific inquiry is to build explanatory theory about its data. In this view, the aim is to explain the data, not just to use the data for description" (Punch 2005, 14). Explanation goes further than description and "involves finding the reasons for things, events and situations, showing why and how they have come to what they are" (Punch 2005, 14). Social Research without theoretical grounding can only describe a situation. Anyway, a good description of exactly what happens takes the place of speculation and impression and is a decisive first step and the basis for explanation (Punch 2005, 15; Babbie 2010, 19).

Therefore, theory has a prominent role in our overall study design. It is with the help of theory that we will explain the findings and, in turn, the data should test and verify our theory.

The aim of our study is not only to describe how users perceive privacy and surveillance on social networking sites, but also to explain why they do as they do.

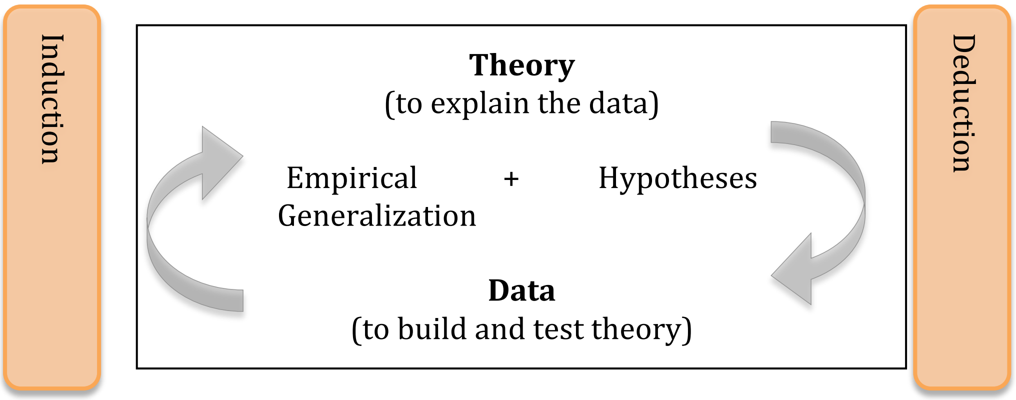


Figure 2: Theory and Data (Punch 2005, 12, Babbie 210, 23)

Our study is based on a theory as a starting point, from which hypotheses are deduced; these consequently are tested in the empirical study. This mode of inquiry is known as deduction or deductive reasoning, moving from the general to the specific. From a general pattern that might be logically or theoretically expected, it moves to observations that whether the expected pattern actually occurs (Babbie 2010, 23). Such an approach is also called "theory verification" (Punch 2005, 16) or "theory first" (Wolcott 1992). However, many authors (Punch 2005, 17; Glaser and Strauss 1967; Brewer and Hunter 1989) are critical of verification as "the keynote of current sociology" (Glaser and Strauss 1967, 10). They argue that the emphasis on verification of existing theories keeps researchers from investigating new problem areas (Punch 2005, 17).

Since the theory applied here, is based on a critical understanding of privacy & surveillance and frames these phenomena in a critical and thereby innovative way, this reproach does not apply.

The relation between theory and data within our study will be bidirectional and iterative. Conducting both, quantitative and qualitative research, as well as taking into account existing pre-study (Fuchs 2009), theory will evolve and advance.

Howcroft and Trauth (2005, 43) emphasize that the dialectic of theory and practice calls for empirical work. They refer to the Frankfurt School thought by stating that "a truly critical theory ... is not restricted to pure thought and critical theorists are never satisfied with merely increasing knowledge (Horkheimer 1931/1972). Instead, a truly critical theory is involved with the present social conditions and materializes by employing the conception of reason as a 'critical tribunal' (Marcuse 1968, 136)".

Adorno (1976, 69) underlines the importance of combining critical theory with empirical research: critical theory "must transform the concepts which it brings, as it were, from outside into those which the object has of itself, into what the object, left to itself, seeks to be, and confront it with what it is. It must dissolve the rigidity of the temporally and spatially fixed object into a field of tension of the possible and the real: each one, in order to exist, is dependent upon the other. In other words, theory is indisputably critical. But, for this reason, hypotheses derived from it – forecasts of what can be regularly expected – are not completely sufficient for it. What can merely be expected is itself a piece of societal activity, and is incommensurable with the goal of criticism. The cheap satisfaction that things actually come about in the manner, which the theory of society had suspected, ought not to delude the theory, that, as soon as it appears as a hypothesis, it alters its inner composition. The isolated observation through which it is verified belongs, in turn, to the context of delusion, which it desires to penetrate. The concretization and certainty gained must be paid for with a loss in penetrating force; as far as the principle is concerned it will be reduced to the phenomenon against which it is tested. But if, conversely, one wishes to proceed in accordance with general scientific custom from individual investigations to the totality of society then one gains, at best, classificatory higher concepts, but not those which express the life of society itself".

According to Adorno, theory and empirical research are contradictory, just like contemporary society itself is. But "it is not a matter of smoothing out such divergences and harmonizing them. Only a harmonistic view of society could induce to such an attempt. Instead, the tension must be brought to a head in a fruitful manner" (Adorno 1976, 70).

Even Marx already stated that "all of science would be superfluous", if there were no difference between things as they appear and things as they actually are (Marx und Engels 1987, 25:384).

In setting up research questions #3 and hypotheses #8-11 (see section 2) we strove for a value-conscious, clear and transparent argumentation, in order to develop a conceptual framework that allows evaluating reliable and comparable data. However, these hypotheses are informed by critical theory (Horkheimer, 245–294; Horkheimer and Marcuse, 625–647). Other social researchers, such as Babbie, put typical positivist views forward that emphasizes that "scientific theory – and more broadly, science itself – cannot settle debates about values" (Babbie 2010, 11). The phrase "value-free sociology" was coined by Max Weber (Weber 1958, 129–56) and urged that a researcher's personal value should not interfere with or influence scientific research. However, we do not agree with such viewpoint. We argue that social science and social action cannot and should not be separated. Critical empirical research aims at creating knowledge as a catalyst for change, helping and giving voice to various marginalized groups and stakeholder, playing an active role in transforming practices and social relations, and assisting actors in emancipating themselves (Österle et al. 2005). "This is based on the belief in the power of knowledge – ideally co-produced by researchers and participants in the study – to transform consciousness of actors about their position and ability to act thus engendering action. It is also based on the conviction that it is not only legitimate but that it is indeed an obligation for a researcher to actively engage in the transformation of … practices" (Cecez-Kecmanovic 2007, 1447). As Babbie (2010, 78) points out that some scholars contend, we agree that "explanations of the status quo in society … shade subtly into defense of that same status quo." In our view, opposed to the positivist view, science is not value-free (see for more Adorno 1976, 68-86; Sevignani et al. 2011, 69-75). Therefore seeing "facts and values as quite different things" is a "mistaken dualism" (Punch 2005, 47). Unaware of its social determination " theory was absolutized … and became a reified, ideological category" (Horkheimer 1972, 194). "The scholar and his science are incorporated into the apparatus of society: his achievements are a factor in the conservation and continuous renewal of the existing state of affairs, no matter what fine names he gives to what he does" (Horkheimer 1972, 196). Kellner infers that "traditional theory … is unaware of the ways in which it is bound together with social processes and thus fails to see its lack of autonomy and social determination" (Kellner 1990, 21).

Babbie (2010, 80), in this context and clearly from a positivist standpoint, states: "Although the abstract model of science is divorced from ideology, the practice of science is not." Punch (2005) argues that value judgements should not be used in instrumental questions, but can occur in the terminal value sense (Punch 2005, 48). However he suggests that "we should indicate how the evidence will be used in conjunction with the value judgements." (Punch 2005, 48)

Therefore we agree that phrasing of research questions and hypotheses should be done careful and any value judgements have to be recognized and clearly stated and argued. The same applies to any data collection questions. However, though on the content level our data collection questions are informed by critical theory, they should be phrased in a neutral way. Otherwise they may convey a suggestive impression and validity of empirical data may get affected.

1.1 Research Topic & General Research Questions

Our research project aims at studying attitudes of Austrian students towards privacy and mechanisms of surveillance on social networking sites. Therefore the crucial concepts here are:

- Privacy
- Surveillance
- Social Networking Sites (SNS)

1.1.1 Privacy & Surveillance

As already outlined in other project publications (Fuchs 2009; Fuchs 2011d; Fuchs 2011e; Sevignani et al. 2011; Allmer 2010a; Allmer 2010b; Kreilinger 2010; Sevignani 2011; Fuchs 2010a; Fuchs 2010b; Fuchs 2010c; Fuchs 2011a), we explicitly conduct privacy- and surveillance studies from a critical theory point of view. Summarizing our existing theoretical approaches to privacy and surveillance, decisive for the conceptual framework are the following assumptions:

- we focus on informational privacy (Tavani 2008; Tavani 1999) since we are exploring privacy issues in context of social networking sites that are based on personal information
- we lay our main emphasis on economic surveillance (for example see Fuchs 2011c; Fuchs 2010a; Fuchs 2010b; Fuchs 2010c) i.e. the aggregation, collection, usage, selling of user data by economic actors in order to gain profit.
- we take a critical stance at surveillance. It is a concept based on domination, coercion, and oppression (Foucault 1975).
- we take a critical stance towards the notion of privacy, which are closely linked to concepts of liberal democracy and private property (Lyon 1994; Fuchs 2011a; Allmer 2010b; Kreilinger 2010; Sevignani 2011).

1.1.2 Social Networking Sites

Social Networking Sites are websites that allow individuals to create and share a public profile within a bounded system, and to establish connections and interact with other users (boyd and Ellison 2007). Social networking sites connect people, allow them to keep in touch with friends, upload and share photos, music and videos, provide and share links, interests or even résumés and job applications.

Examples for popular social networking sites are Facebook, MySpace, and Xing. Overall, hundreds of different social networking platforms exist, built around different themes (such as student experience, music, career, love, nationality, culture, hobbies, parentship and so forth) and serving a wide range of interests and lifestyles. However, with more than 800million users, Facebook is arguably the most dominant Social Networking Site, especially in the USA and Europe.

Since their introduction such sites have attracted millions of users, many of whom have integrated these sites into their daily practices (boyd and Ellison 2007). For example, one of the most popular and widespread social networking sites Facebook claims to have attracted over 500 million active users (www.facebook.com/press/info.php?statistics, accessed April 2011).

"The business model of most commercial web 2.0 platforms is based on personalized advertising. Capital is accumulated by selling space for advertisements as well as by selling user data to third-party advertising companies." (Fuchs 2011b)

In context of such practices, Fuchs (2010d; 2011d) stresses the exploitation of users: "New media corporations do not (or hardly) pay the users for the production of content. One accumulation strategy is to give them free access to services and platforms, let them produce content, and to accumulate a large number of produsers that are sold as a commodity to third-party advertisers." (Fuchs 2011c, 287)

In Austria the most commonly used social networking site at the moment is Facebook. It ranks second in the national ranking by alexa.com (January 2012) just behind the search engine Google. Other top ranked social networking sites are Twitter (#15), Xing (#24), LinkedIn (#35) (alexa.com, January 2012). Many other top ranked sites have implemented elements of social networking sites as well. So for example sites such as youtube.com (#3), Wikipedia (#6), blogspot.com (#11), or Flickr (#49) are based on user generated content and the interaction between users.

For the purpose of our survey, however, we will focus on the top ranked social networking sites, especially Facebook. Selection criterion will be the national alexa.com rank, which is one of the most reliable ranking tools, that is publicly available.

2. Conceptualization

2.1 Research Method

Punch (2005, 4) stresses that "methods should follow from questions." He especially criticizes quantitative approaches for " the idolatry of method", "called methodolatry" (Punch 2005, 4, 20). In contrast Punch argues for a "question-to-method influence … , because of its value in ensuring a close fit between the research questions and the methods" (Punch 2005, 5). Punch emphasizes that the content of research should have a logical priority over the method of research. Methods are primarily tools used for answering research questions (Punch 2005, 20–21). However he acknowledges the "reciprocal interaction between question and method." (Punch 2005, 5)

For the third part of our study (Research Question #3 and Hypotheses #8-11), we have chosen quantitative research and will conduct an online survey. Babbie highlights that quantification makes observations more explicit, as well as easier to aggregate, compare, and summarize data. On the other hand, he also points to the disadvantage of numerical data, which might be a potential loss in richness of meaning (Babbie 2010, 24).

2.2 Research Questions

The development of a series of empirical research questions as part of pre-empirical work is important in setting up the research. The aim is to clarify and disentangle the different issues involved (Punch 2005, 4).

According to Punch (2005, 37) research questions do five main things:

- organize the project, give direction and coherence
- delimit the project, showing boundaries
- keep the researcher focused during the project
- provide a framework (for documentation)
- point to the needed data

Good research questions are substantial for conducting good research. Therefore, in developing our research question, we checked if each of them fulfils the attributes required for a good research question. For Punch (2005, 46) these are:

Checklist:

- ✓ clear (easily understood, unambiguous)
- ✓ specific (in order to connect to data indicators)
- ✓ answerable (one can see which data are required to answer them and how the data will be obtained)
- ✓ interconnected (related in some meaningful way)
- ✓ substantively relevant

As part of our study we want to find out how large students' knowledge of surveillance is in general, which attitudes they have towards surveillance and privacy, how much knowledge they have about concrete social networking sites and their individual information behaviour in context of those social networking sites. In analysing this data we want to explore how these variables are correlated. Accordingly, for the 3rd part of our study the research question is:

RQ 3: Are knowledge and attitude towards surveillance and privacy of Austrian students and their information behaviour on social networking platforms connected?

Several studies have already – at least to some extent - explored the relation between knowledge, attitude and behaviour (Acquisti and Gross 2006; boyd and Hargittai 2010; Buchanan et al. 2007; Christofides, Muise, and Desmarais 2009; Dwyer 2007; Fuchs 2009; Hiltz, Passerini, and Dwyer 2007; Hinduja and Patchin 2008; Fogel and Nehmad 2009; Lewis, Kaufman, and Christakis 2008). However these studies focused on individual surveillance and privacy concerns and did not take economic aspects of surveillance and privacy on social networking sites into account. Advertising mechanisms such as behavioural targeting or social advertising and their influence on surveillance and privacy attitudes, as well as advertising settings will be examined in our study.

2.3 Hypotheses

Different definitions of what a hypothesis is exist. For example for Punch a hypothesis simply is "a predicted answer to a research question" (Punch 2005, 38). Other definitions may be: "A hypothesis is a proposition to be tested or a tentative statement of a relationship between two variables. Hypotheses are guesses about how the social world works." (Neuman 2006, 92–93)

As a basis for answering a research question a priori, i.e. framing a hypothesis, Punch (2005, 38) highlights two cases:

a) it is based on the findings of similar research

b) a set of propositions explain the predicted answer. Such set of propositions is a theory.

However, Punch (Punch 2005, 38), emphasizes that though the first case (existing similar findings) do suggest that a certain answer can be expected, it does not provide an explanation why a certain answer can be expected. This can only be accomplished by a theory, from which hypotheses are deducted. This is the classical hypothetico-deductive research model (Punch 2005, 38).

Punch points out that hypothesis are only appropriate "when we do have an explanation (a theory) in mind behind our hypotheses. If this is the case, we should by all means formulate hypotheses as predicted answers to research questions, and test them." (Punch 2005, 38)

Therefore for Research Question #3 we have formulated four hypotheses:

Hypothesis 8: More knowledge about surveillance is significantly positively correlated to more careful information behaviour on SNS (intensity of reading the terms of use, degree of deactivation of advertising options, degree of activation of privacy mechanisms).

Hypothesis 9: A more critical attitude towards surveillance is significantly positively correlated to more careful information behaviour on SNS (intensity of reading the terms of use, degree of deactivation of advertising options, degree of activation of privacy mechanisms).

Hypothesis 10: There are significant differences in information behaviour on SNS between students in the hard and the soft sciences.

Hypothesis 11: A higher degree of privacy concerns is significantly positive correlated to a more careful information behaviour on SNS (intensity of reading the terms of use, degree of deactivation of advertising options, degree of activation of privacy mechanisms).

In the following we will explain each hypothesis and outline its theoretical foundation as well as comparable empirical findings. In order to clarify its meaning, for each hypothesis, all variables involved will be identified. Anticipating step 3 of the research design, i.e. operationalization, we will explain each variable, and point out how it can be measured. Therefore we will draft possible data collection questions, indexes and scales.

Because all four hypotheses aim at assessing the information behaviour of Austrian students on social networking sites, we will start by examining how this variable is conceptualized and will already point out some possibilities to operationalize it (anticipating section 3).

Furthermore, three of the four hypotheses (#8, #9, #11) are theoretically based on the assumption that human behaviour is affected by knowledge/experience and attitudes/concerns (among other factors such as genetics, social norms, core faith). Similarly, changes in behaviour result from knowledge and attitudinal changes. These theoretical assumptions are well documented and explained for example in Parrish (2009), Blackburn (2003) or Ajzen (1988).

2.4 Population and Sampling

A pre-study, conducted by Fuchs (2009) at the University of Salzburg shows that 96.6% of participants (N=639) use social networking sites. Students not only appear to be early adopters of information and communication technologies, but also to fall into the category of "heavy users". Not coincidentally, social networking sites such as Facebook or studiVz were developed in university-context and first established them among the studentship, before also attracting non-student users. Additionally, statistics concerning "user age distribution on Facebook in Austria" show that over 50% of the users are aged between 18 and 34 (www.socialbakers.com, retrieved January 2012).

Therefore our population are Austrian students. We assume anyone officially enrolled in one of Austria's public universities to be considered an Austrian student. These are:

- Akademie der bildenden Künste Wien
- Alpen-Adria Universität Klagenfurt
- Johannes-Kepler Universität Linz
- Karl-Franzens-Universität Graz
- Leopold-Franzens-Universität Innsbruck
- Medizinische Universität Graz
- Medizinische Universität Innsbruck
- Paris-Lodron Universität Salzburg
- Technische Universität Graz
- Technische Universität Wien
- Universität für angewandte Kunst Wien
- Universität für Bodenkultur Wien
- Universität für Musik und darstellende Kunst Wien
- Universität Mozarteum Salzburg
- Universität Wien
- Veterinärmedizinische Universität Wien
- Wirtschaftsuniversität Wien

3. Data Collection

In order to answer our research questions, we conducted a quantitative online survey among Austrian students.

Within the social research literature advantages and disadvantages of online surveys are widely discussed (see for example Babbie 2010, 283–287; Wright 2005; Couper 2001; Kaplowitz, Hadlock, und Levine 2004; Ilieva, Baron, und Healey 2002; Evans und Mathur 2005; Yun und Trumbo 2000; Lefever, Dal, und Matthíasdóttir 2007). Typical advantages highlighted in the literature are:

+ fast/improved response time: in the course of our study we have always been able to observe, if and when an announcement of the survey was sent to students, because response rates immediately soared up; after two to three days responses slowed down again.

+ improved scope of the survey: the form of an online survey allowed us to reach more students than other/traditional survey tools would have allowed for: with an online survey there is no difference whether one aims for 100 or 1,000 respondents.

+ less resource-intensive: in contrast to a phone survey or an in-person survey it is possible to reach a high response rate with reasonable expenditure (time, money, personnel,…).

+ relatively inexpensive: once the survey has been constructed, it is rather inexpensive to administer it.

+ facilitates data analysis: since the results are already digital and can usually be exported from the online survey tool in the format needed for further analysis encoding and tabulating effort can be reduced. Thus it makes collecting and analysing responses easy and accurate. The results can be easily converted to graphic representations.

+ more flexibility:

- form: e.g. we were able to insert screenshots in order to give clear instructions as well as impressions (e.g. about Facebook's privacy settings)
- changes: the online survey instrument allowed us to adapt the survey, in case it became necessary. So for example it allowed us to adjust screenshots, when Facebook has made some minor changes in its screen design.
- Question logic: depending on preceding answers, different sets of questions were presented to the participant. For example, if someone has never heard of the "Network Advertising Initiative" that allows to opt out from cookies being placed on his/her computer, there would be no need to bother him/her with further/more detailed questions about it (Questions 62-65)

+ less disruptive: people can complete online surveys on their own schedule. Therefore an online survey is less disruptive than an in-person or phone survey.

+ respondents are usually more willing to answer questions about sensitive topics when replying to a computer rather than a person. Additionally, answers tend to be more honest.

+ no media discontinuity: in order to answer some of our research questions we asked respondents to look up their privacy settings on Facebook. This was only possible because respondents already were on their computers and online when answering the questionnaire. Thus, they only needed to make some clicks, instead of switching between different media.

Typical disadvantages highlighted in the literature are:

- scope limited to Internet users: In this context, Babbie (2010, 284) stated: "people who are less available to online surveys do not represent a random segment of the overall population. The poor and the elderly, for example, are likely to be underrepresented in online surveys. At the same time, as more and more people gain access to the Internet, this problem will decline (An early criticism of telephone surveys was that not everyone had a phone.)"

For our survey, the target group represents an age group that usually already has grown up with the Internet and can even be described as "heavy users" (students are even somehow forced to use the internet: organizational tasks like course enrolment often need to be fulfilled online; writing seminar papers or making presentations usually also call for online research). According to a survey conducted by Statistik Austria in 2011 among the 16-to-24 year olds in Austria 98.1% have used the Internet in the last three-month, 99.2% have used it in the last year (Statistik Austria 2011)

Also the research questions are centred around an online phenomena: Social Networking Sites. Therefore, students, who actually do not use the Internet, would unanimously be non-users of such platforms and thus be of no interest for our survey.

- possibility of multiple data entry: it is possible that the same person completes the survey twice or even more often. Since our survey is rather long and respondents approximately needed 20-30 minutes for finishing it, we do not assume this to be a considerable problem.

- lower response rate: especially by comparison with in-person surveys. However, results are comparable to mail surveys: "online surveys appear to have response rates approximately comparable to mail surveys, according to a large scale study of Michigan University students" (Babbie 2010, 285). Although in-person surveys would have had better response rates, such an approach would have been limited due to restricted resources. Therefore using an online survey allowed us to contact far more people than any other method would have.

Punch (2005, 100) highlights that "it is necessary to ensure that respondents have been approached professionally and, within limits, fully informed about the purpose and context of the research, about confidentiality and anonymity, and about what use will be made, and by whom, of the information they provide. It helps also to point out that this sort of research is not possible without their cooperation, and they should know clearly what they are being asked to do. Experience shows that when this is done properly and professionally, people will cooperate and the quality of the data is improved." We heeded this advice and included the following starting page for our survey:

The Usage of Social Networking Sites by Students in Austria

The Unified Theory of Information (UTI) Research Group conducts a study of Austrian students' usage behaviour of social networking platforms (Facebook, studiVZ, MySpace, etc). We appreciate if you can help is in this research by filling out a questionnaire. Completing the survey will take approximately 20 minutes. All data is treated confidentially and anonymously.

We will give away Amazon vouchers with a total value of 1,000€ (1x500€, 2x100€, 30x10€) in a lottery among the participants. Supplying your email-address is voluntary and the address will be stored independently of your survey data. It is also possible to participate in the survey without taking part in the lottery. To be considered for the lottery you need to answer all questions.

It would be of great help to us, if you inform your friends, who also use social networking sites, such as Facebook, about this survey. The more fully completed questionnaires we receive, the better results we will obtain.

Reports on the results of the survey will be published subsequently.

Contact:
Prof. Christian Fuchs (Projektkoordination)
UTI – Unified Theory of Information Research Group
Steinbrechergasse 15
1220 Wien
survey@uti.at
http://www.uti.at

UTI. Unified Theory of Information Research Group

Babbie (2010, 284-285) provides another advice that we did consider: "do offer to share selected results from the study with everyone who completes the survey. Respondents will often welcome information as a reward for taking the study, especially when they are young adults and teens"

Thank you for participating in this study. Your answers are important for us in order to advance research about social networking.
[…]
If you want to receive updates on research reports that result from this project, then enter your email address.

Additionally to providing final research reports to the participants, we gave away Amazon vouchers in a lottery. As Babbie (2010, 285) suggests, that "longer surveys usually require larger incentives", we offered vouchers with a total value of 1,000€, adding up 1x500€, 2x100€ and 30x10€ vouchers. Any participant of the study, who had answered the entire questionnaire, was considered for the lottery. In order to avoid any ethical problems, we stored the email-addresses,

We will give away Amazon vouchers with a total value of 1,000€ (1x500€, 2x100€, 30x10€) in a lottery among the participants. Supplying your email-address is voluntary and the address will be stored independently of your survey data. It is also possible to participate in the survey without taking part in the lottery. To be considered for the lottery you need to answer all questions.

needed for contacting the winners, separately from the data files. The lottery was promoted with the following announcements at the beginning, as well as at the end of the questionnaire:

> If you want to take part in winning one of the Amazon vouchers, then please enter your email address. It will be stored independently of your answers.
> If you want to receive updates on research reports that result from this project, then enter your email address.
> Q78: You can leave the following field blank.
> - participate in the lottery
> - receive information on research reports
> - not specified
> - email-address:
>
> The winners of the vouchers are drawn randomly after the survey ends. They will be notified per email.

For conducting the survey we decided to use the online tool “surveymonkey.com”. In comparison to other tools it offered a reasonable price and appeared to be a user-friendly software. When programming the survey we tried to make sure that the survey was easy to navigate and to answer.

The research was carried out from June to November 2011. The questionnaire was available for 157 days. Our potential respondents were students in Austria. In order to reach them we sent out invitation to participate with the help of University Administrations, University’s Public Relations Departments and the “ÖH- Österreichische HochschülerInnenschaft” (official representation of Austrian university students). We asked local platforms and online forums that are frequently used by students to post invitations. We posted announcements of the survey on different Facebook Sites and discussion groups. Additionally, for a short period in June and July we promoted the survey on Facebook as well as on Google (Google AdWords).

Our potential respondents were male and female students at all 22 universities in Austria. This included students of all fields of studies and of all age groups independent from study progress (bachelor, master, phd- students).

In total 5,213 students responded to the announcement of the survey and started the questionnaire. 84.8% or 4,419 students actually finished the questionnaire. According to the Austrian Federal Ministry for Science and research there were in total 273,542 students enrolled at 22 universities in Austria in 2011. Therefore 1.91% of the total population responded to the survey, 1.62% completed the questionnaire and thereby represent our sample size for further data analysis.

4. Operationalization of the Variables & Indices, Data Analysis & Results

According to Punch (2005, 45), in quantitative research, connecting a concept to its empirical indicators is called operationalism. Research questions and prespecified hypotheses should give clear indications of the data needed to answer and test them. So for the quantitative part of the study, the linking of concepts and data is done ahead of the empirical stage. Punch refers to this order as a link "from concepts to data", in which the "variables are operationally defined" (Punch 2005, 46). In order to explore relations between objects, variables are defined. Variables are logical sets of attributes, which in turn are characteristics or qualities that describe an object (Babbie 2010, 14–15). For answering Research Question #3, the following variables need to be assessed:

Variable #1: Information Behaviour

Variable #2: Surveillance Knowledge

Variable #3: Critical Attitude towards Surveillance

Variable #4: Field of Study (Hard Science & Soft Science)

Variable #5: Privacy Concerns

In order to operationalize these variables, we first need to be explicit about what the concept actually means in our research context. Babbie (2010, 25) points out that "by focusing specifically on what we'll include in our measurement of the concept, however, we also exclude any other meanings." For the definition and clarification of each variable, see the respective section within 2.3 Hypotheses.

Since the quantitative study is prespecified in contrast to an unfolding research structure, data are structured in advance. Pre-established categories and measurement is used to give the data numerical structure a priori (Punch 2005, 24). Because it is a quantitative survey it is necessary to quantify a nonnumerical concept such as "critical attitude towards surveillance". As already outlined in section 2.3 we will create or use existing indexes in order to quantify variables such as "surveillance knowledge", "critical attitude towards surveillance" and "privacy concerns". These indexes will allow us to observe relationships between the concepts.

Therefore we have to carefully assess the relation between the independent and dependent variables. As a checklist, Punch's list (Punch 2005, 49) of the main conditions for inferring a causal relationship between two variables (X and Y), can be helpful:

- ✓ "The variables X and Y must be related"
- ✓ "A time order between the variables must be demonstrated, with the cause X preceding the effect Y."

- ✓ "There must be a plausible theory showing the links by which the variables are causally related: that is, the missing links which bring about the causal connection must be specified."
- ✓ "Plausible rival hypotheses to the preferred causal one must be eliminated."

Of course such assumption is somewhat oversimplified, since in research practice multiple causation is much more realistic (Punch 2005, 51). The most common design in quantitative research usually is multiple causes/one effect design (Punch 2005, 52). As for the quantitative part of our research this holds true. In Hypothesis 8, 9, 10 and 11, for one effect (more careful information behaviour on SNS) multiple causes (more knowledge about surveillance, a more critical attitude towards surveillance, field of study, and a higher degree of privacy concerns) are predicted. Figure 3 summarizes the relationship between the five variables, we will operationalize for answering research question #3.

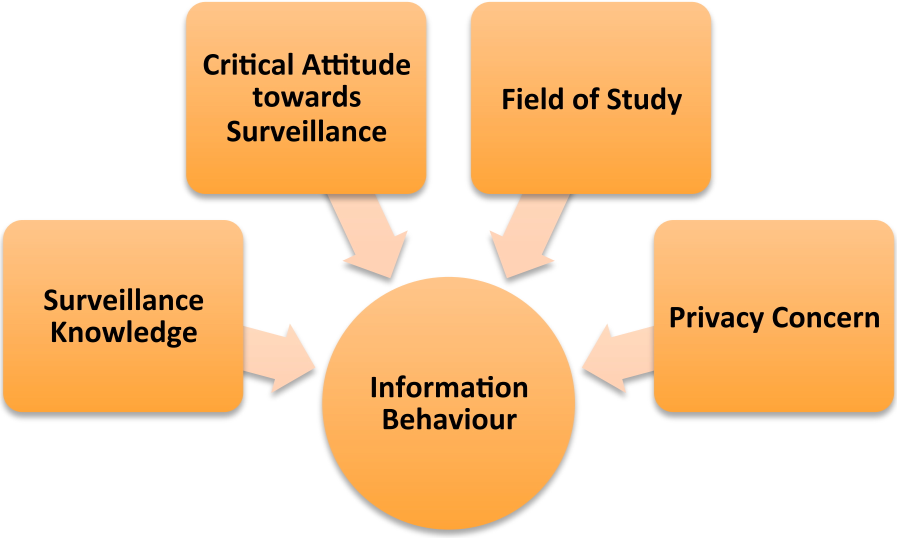


Figure 3: Relationship between Variables

4.1 Variable #1: Information Behaviour

"Information behaviour is the currently preferred term used to describe the many ways in which human beings interact with information, in particular, the ways in which people seek and utilize information" (Bates 2010, 2381).

Research on information behaviour is concerned with "how individuals approach and handle information. This includes searching for it, using it, modifying it, sharing it, hoarding it, even ignoring it" (Davenport 1997, 83).

In our research we are interested in understanding the human relationship with personal information, and its affection by surveillance mechanisms in the context of social networking sites. It is this relationship that defines and builds the web 2.0 environment. However it is not a relationship between equals. As highlighted above (see section 1), social networking sites are based on the collection and sale of personal information of their users. Other threats to information privacy may be posed upon users by potential state surveillance or harmful individuals.

Therefore users of social networking sites should bear in mind possible disadvantages they may encounter when sharing personal information online. Our aim is to explore how exactly users interact with social networking sites in terms of their information behaviour.

Several studies already aimed at examining user's information behaviour. For example Christofides, Muise, and Desmarais (2009) asked participants survey questions such as "How likely are you to say no to a Facebook friend's request in order to control who has access to your information". However, such questions can only explore users' information behaviour fragmentarily. Considering the profit-oriented character social networking platforms such as Facebook have, profile settings (in order to control access to one's profile) alone do not give users control over their personal data. Platform providers can still collect, process, use, and sell the personal information of their users. Therefore, in order to get a broader view, we will also analyse if and to what extent users protect their personal data from economic actors e.g. if they use opt-out solutions of targeted advertising (if available), or how they interact with advertisements displayed on social networking sites or other marketing efforts such as groups or fanpages/sites.

The extent to which a person's information behaviour may be considered careful depends upon different actions. In order to operationalize general "Information Behaviour", we posed questions within five sub-categories:

- General Usage,
- Shared Information,
- Access,

- Privacy Settings,
- Advertising

Hence, we were able to explore the many dimensions of respondents' information behaviour and were also able to check for differences between these categories. In the questionnaire we presented 21 items (4 items for each subcategory, 5 items for "general usage") to the participants:

General Usage

1. How often do you upload pictures to social networking sites, in order to share them with others?
2. How often do you upload videos to social networking sites, in order to share them with others?
3. How often do you share a comment or status on social networking sites?
4. How often do you write messages or chat with other users on social networking sites?
5. How often do you use Facebook?

Shared Information

5. Do you use your real name or a pseudonym on Facebook?
6. Are your clearly identifiable on your Facebook profile picture?
7. Does someone share pictures? (Retrieved from Q1)
8. Does someone share comments/status updates? (Retrieved from Q3)

Access

9. How many Facebook friends do you have?]
10. Are any Co-workers among your Facebook friends?
11. Are any superiors/bosses among your Facebook friends?
12. Are any Professors/Lecturers among your Facebook friends?

Privacy Settings

13. Which privacy settings have you chosen for Facebook?
14: When you join or use a social networking site, do you read the privacy policy and terms of service?
15: Have you ever changed the default privacy settings for Facebook? If yes, how often?
16. Have you ever blocked a Facebook Application (as e.g. birthday calendar, FarmVille, Cities I've visited…), because it accesses your data?

Advertising

17. Have you ever clicked on an advertisement displayed on Facebook?
18. What is your setting that defines whether third parties are allowed to use your name or profile for advertising purposes?

19. What is your setting, that defines whether friends can see which products or services you like?
20. Have you ever joined a group or site that has been established and is run by a commercial actor (e.g. local restaurants or shopping malls, brand communities such as Starbucks, Nike, etc.)?]

The following section will show the results for the single questions:

4.1.1 General Usage

In order to evaluate the general usage of Facebook of the respondents, we asked them to check how often they do the following typical activities on Facebook: share a picture, share a video, update their status or comment, and write a message or chat.

Respondents were asked to rate their answers on a scale ranging from 1 to 8, with 1 meaning “several times a day” and 8 meaning “never”.

Expectedly, respondents most often write messages and update their statuses or comment on other users’ statuses. The Mean for these two questions shows that users on average do these activities between once a week and several times a week. Uploading and sharing pictures is still a very frequent activity, with a mean of 6.5, which indicates that users on average share pictures once a month. Only when it comes to sharing videos, users are less active. 60% of the respondents have never uploaded and shared a video, around 27% do so every now and then (less than once a month), and only around 13% share videos on a regular basis (at least once a month). However, since making a video takes arguably more effort than posting a comment, these figures are still high.

Additionally, we asked respondents how often they use Facebook in general. Results show that over three quarters (77.6%) of the study participants use Facebook once or even several times a day. 13.1% still log onto Facebook several times a week, and only 8.9% use it less often. However, 4% of the respondents stated they use Facebook less often than once a month. These may be users that only tried it out once, or have abandoned the platform.

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Share pictures	3558	1,00	8,00	6,5402	1,16381
Share videos	3558	1,00	8,00	7,3485	1,09358
Status update/comment	3558	1,00	8,00	4,5163	1,87361
Messages/Chat	3558	1,00	8,00	3,4604	1,78504
Valid N (listwise)	3558				

Table 1: Descriptive Statistics for General Usage Items

8-point answering scale:

[1] Several times a day; [2] Once a day; [3] Several times a week; [4] Once a week; [5] Several times a month; [6] Once a month; [7] Less often; [8] Never.

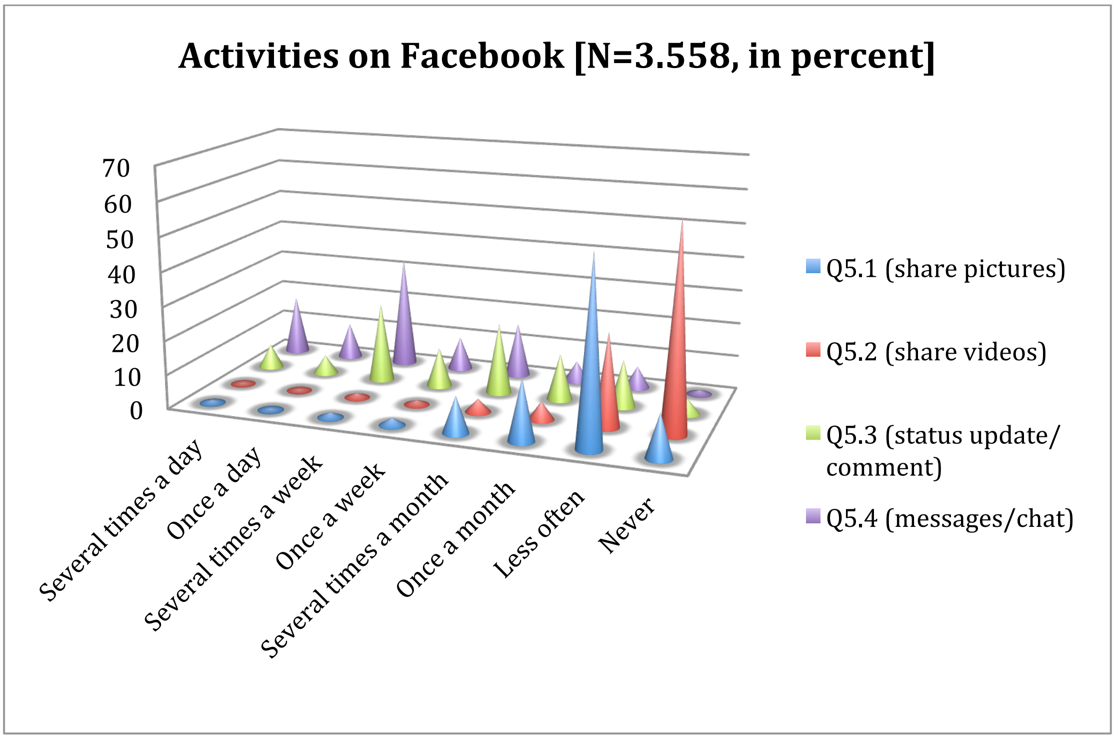


Figure 4: Activities on Facebook (percent)

In the following, the results (percentage and frequency) for each of the five questions are shown in detail. The results are rounded up to one decimal place.

Q5.1 How often do you upload pictures to social networking sites, in order to share them with others?

		Frequency	Percent	Cumulative Percent
Valid	Several times a day	28	,8	,8
	Once a day	17	,5	1,3
	Several times a week	52	1,5	2,7
	Once a week	78	2,2	4,9
	Several times a month	379	10,7	15,6
	Once a month	635	17,8	33,4
	Less often	1917	53,9	87,3
	Never	452	12,7	100,0
	Total	3558	100,0	

Table 2: Results to Question 5.1

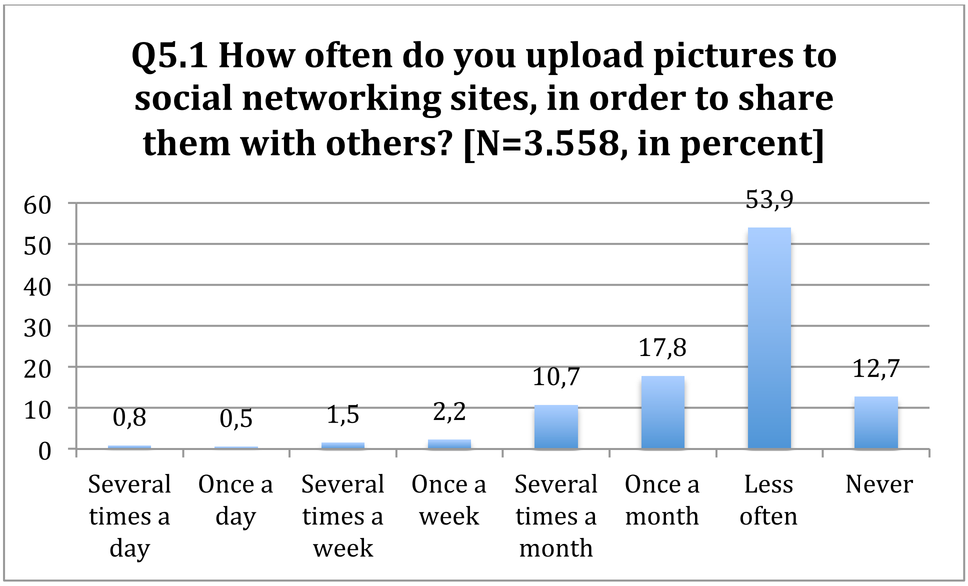


Figure 5: Results to Question 5.1

Q5.2 How often do you upload videos to social networking sites, in order to share them with others?

		Frequency	Percent	Cumulative Percent
Valid	Several times a day	9	,3	,3
	Once a day	12	,3	,6
	Several times a week	47	1,3	1,9
	Once a week	47	1,3	3,2
	Several times a month	138	3,9	7,1
	Once a month	188	5,3	12,4
	Less often	970	27,3	39,7
	Never	2147	60,3	100,0
	Total	3558	100,0	

Table 3: Results to Question 5.2

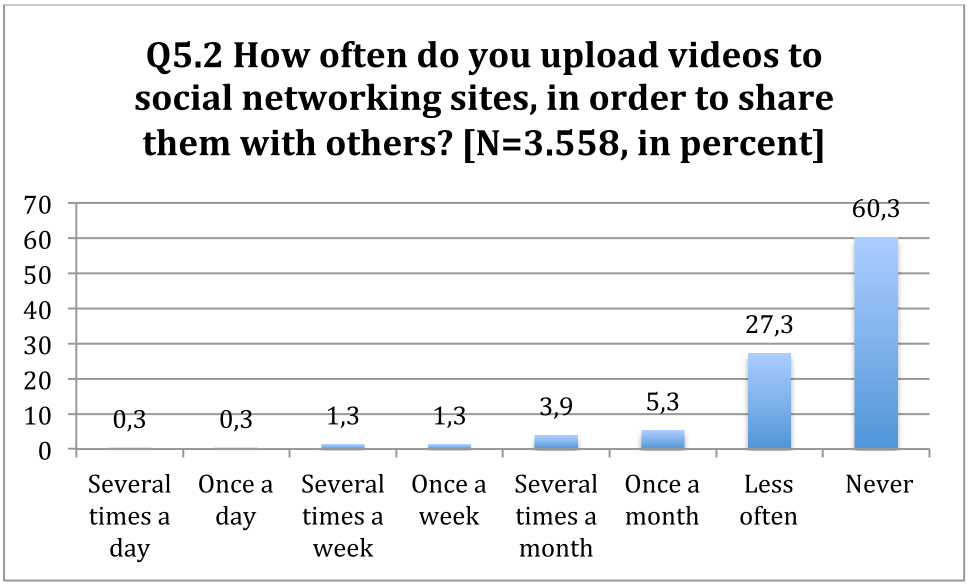


Figure 6: Results to Question 5.2

Q5.3 How often do you share a comment or status on social networking sites?

		Frequency	Percent	Cumulative Percent
Valid	Several times a day	250	7,0	7,0
	Once a day	193	5,4	12,5
	Several times a week	830	23,3	35,8
	Once a week	414	11,6	47,4
	Several times a month	741	20,8	68,2
	Once a month	484	13,6	81,8
	Less often	490	13,8	95,6
	Never	156	4,4	100,0
	Total	3558	100,0	

Table 4: Results to Question 5.3

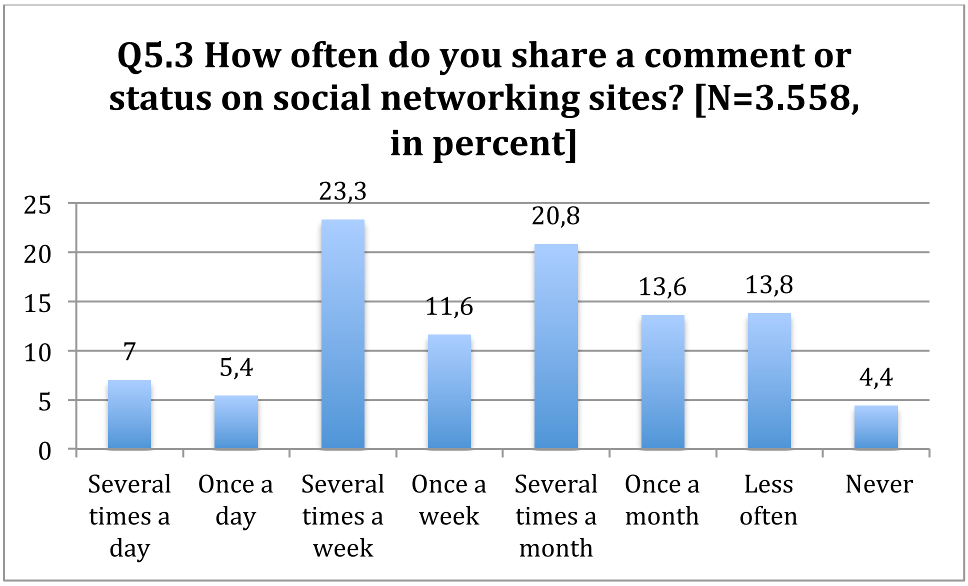


Figure 7: Results to Question 5.3

Q5.4 How often do you write messages or chat with other users on social networking sites?

		Frequency	Percent	Cumulative Percent
Valid	Several times a day	618	17,4	17,4
	Once a day	373	10,5	27,9
	Several times a week	1167	32,8	60,7
	Once a week	350	9,8	70,5
	Several times a month	565	15,9	86,4
	Once a month	215	6,0	92,4
	Less often	228	6,4	98,8
	Never	42	1,2	100,0
	Total	3558	100,0	

Table 5: Results to Question 5.4

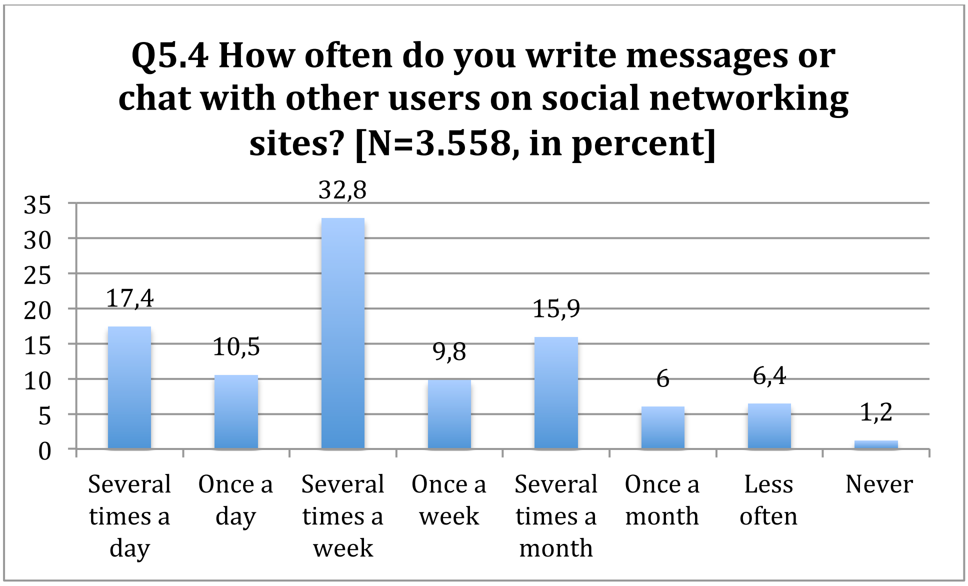


Figure 8: Results to Question 5.4

Q8. How often do you use Facebook?

		Frequency	Percent	Cumulative Percent
Valid	Several times a day	1964	55,2	55,2
	Once a day	796	22,4	77,6
	Several times a week	465	13,1	90,6
	Once a week	95	2,7	93,3
	Several times a month	68	1,9	95,2
	Once a month	29	,8	96,0
	Less often	141	4,0	100,0
	Total	3558	100,0	

Table 6: Results to Question 8

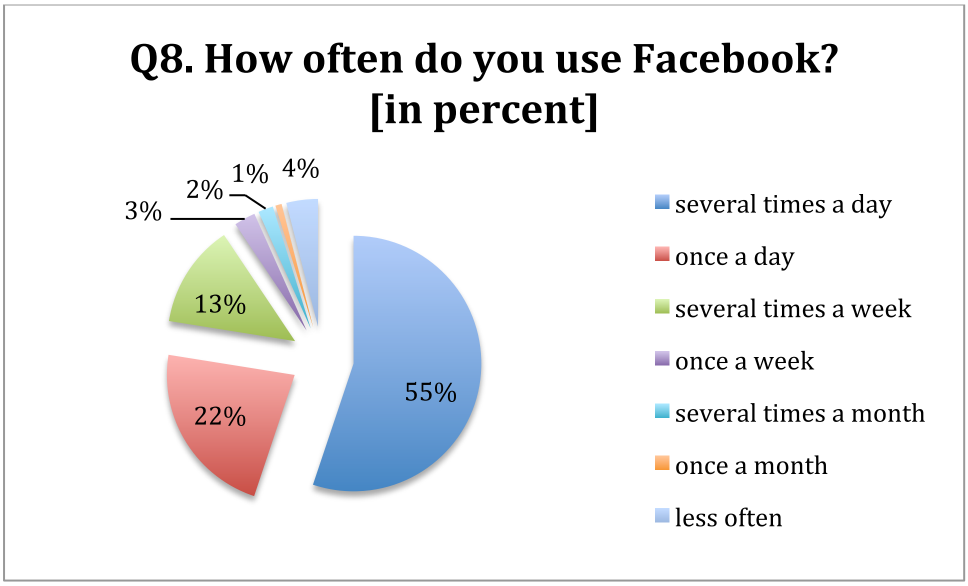


Figure 9: Results to Question 8 (percent)

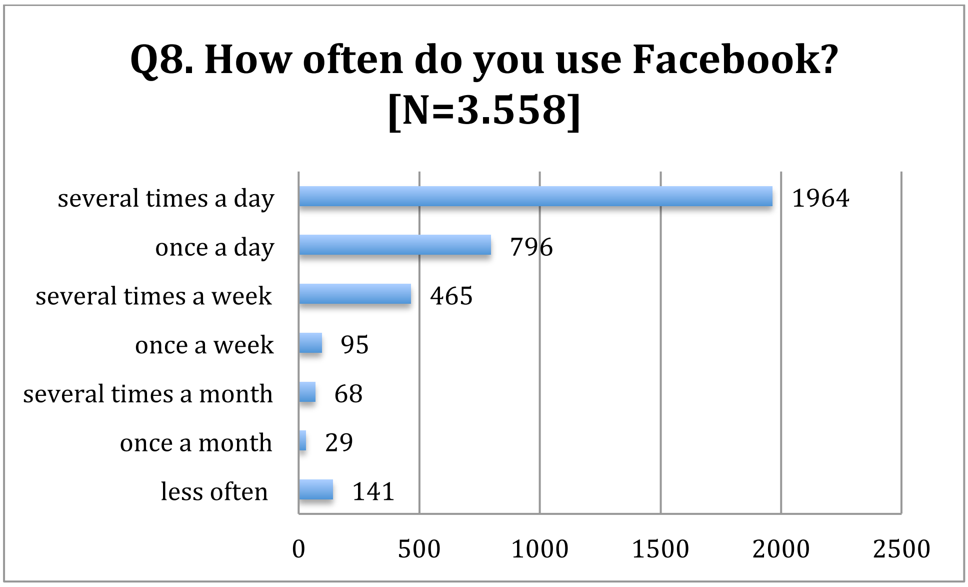


Figure 10: Results to Question 8 (frequency)

4.1.2 Shared Information

In this category we aimed at analysing which kind of information Facebook users share. Therefore we asked respondents if they use their real name or a pseudonym on Facebook and if they have posted a profile picture on which they are clearly identifiable - both information that is public to everyone, no matter what someone's privacy settings are. Especially the usage of a pseudonym or fake name is a highly contested case, since in its name policy Facebook demands users to list their real, full names. This policy reserves Facebook the right to close any account identified using a fake name. In an attempt to check for the real identity of their users names, Facebook even called on their users to report any of their friends who use fake names. Our findings show that in spite of this policy, 20.5% of our respondents use a pseudonym on their Facebook profile. Even more (31.3%) stated no to be clearly identifiable on their profile picture. These results imply that for a great percentage of users preserving their anonymity is important. Only their Facebook friends are allowed to know who is behind a certain profile.

Additionally we checked if respondents share pictures and status updates on their profile page. We assumed that most respondents do, and the results verified this assumption. However, 12.4% do not share any pictures on their Facebook site, and 4.4% do not share any status update or comment on other posts.

In the following, the results (percentage and frequency) for each of the four questions are shown in detail. The results are rounded up to one decimal place.

Q10. Do you use your real name or a pseudonym on Facebook?

		Frequency	Percent	Cumulative Percent
Valid	Name	2830	79,5	79,5
	Pseudonym	728	20,5	100,0
	Total	3558	100,0	

Table 7: Results to Question 10

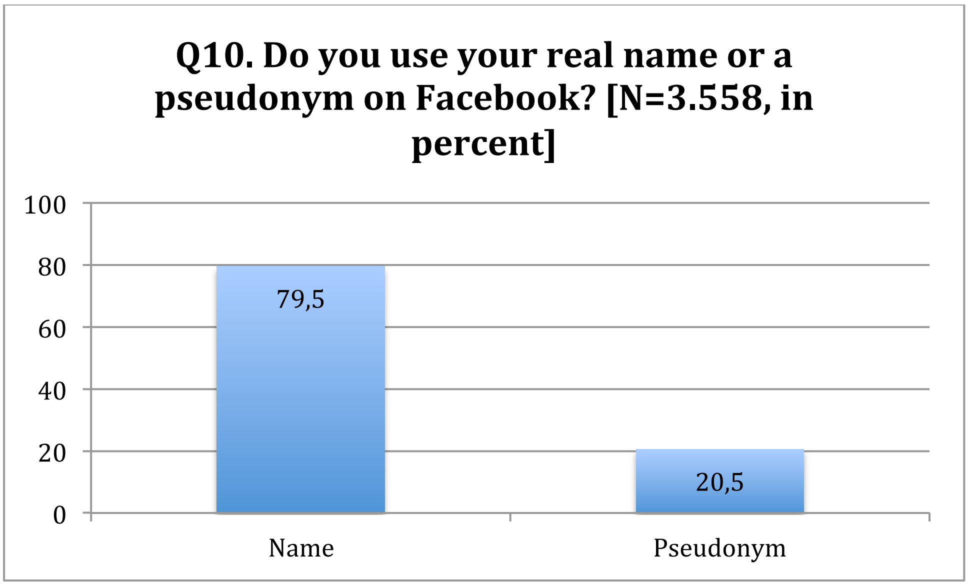


Figure 11: Resukts to Question 10

Q9. Are your clearly identifiable on your Facebook profile picture?

		Frequency	Percent	Cumulative Percent
Valid	Yes	2444	68,7	68,7
	No	1114	31,3	100,0
	Total	3558	100,0	

Table 8: Results to Question 9

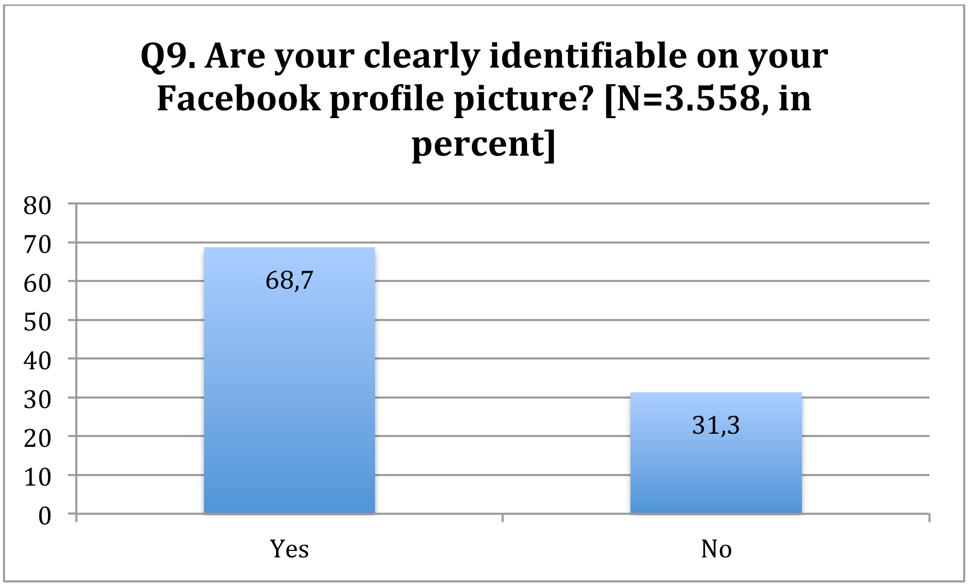


Figure 12: Results to Question 9

Q5_1.1 Does someone share pictures? (Retrieved from Q5.1)

		Frequency	Percent	Cumulative Percent
Valid	Yes	3106	87,3	87,3
	No	452	12,7	100,0
	Total	3558	100,0	

Table 9: Results to Question 5.1.1

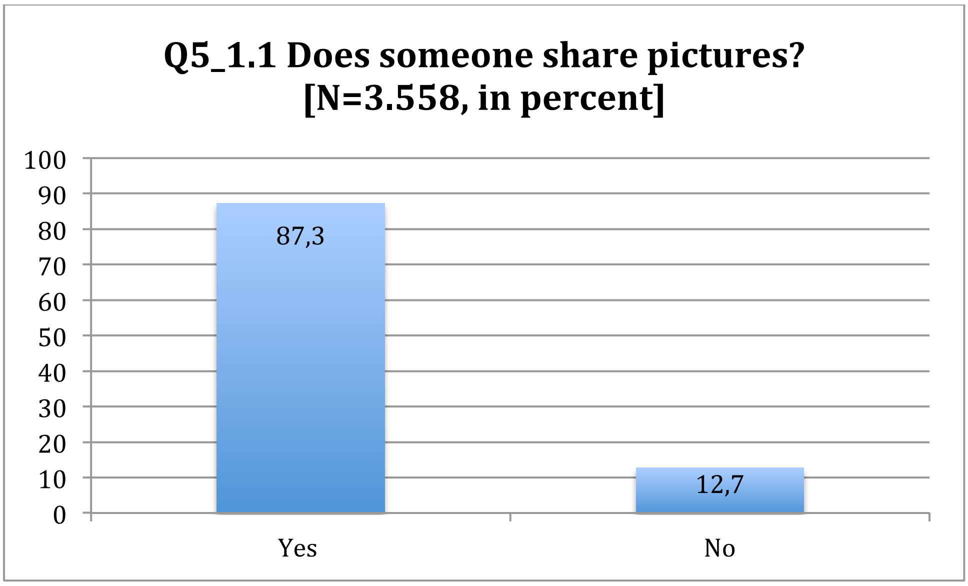


Figure 13: Results to Question 5.1.1

Q5_3.1 Does someone share comments/status updates? (Retrieved from Q5.3)

		Frequency	Percent	Cumulative Percent
Valid	Yes	3402	95,6	95,6
	No	156	4,4	100,0
	Total	3558	100,0	

Table 10: Results to Question 5.3.1

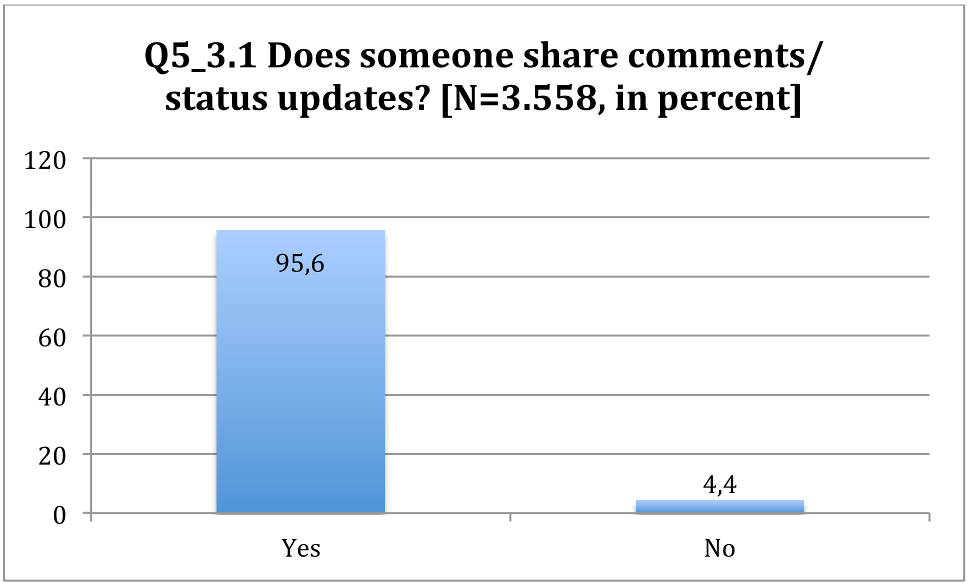


Figure 14: Results to Question 5.3.1

4.1.3 Access

In this section we wanted to find out to whom our respondents give access to their Facebook profiles. The first question asked for the amount of Facebook friends someone has. The results show that the majority of our respondents have between 100 and 299 Facebook friends, around a fifth of our respondents have less than 100 Facebook friends, and 14.6% rank 300-399 other users among their friends on Facebook. Put together, 12.3% of all respondents checked that they have more than 400 friends (with 2.9% having even more than 600 friends), which is quite an astonishing high number. The concept of "friend" seems to be quite different on Facebook than in real life. Additionally, we asked the respondents whether or not they are friends with the following people on Facebook: co-workers, superiors at work, or professors/lecturers. A majority of 77.6% of the respondents are friends with at least some of their co-workers on Facebook. 15.8% have their working superiors, and 13.0% have any professors/lecturers among their Facebook friends.

In the following, the results (percentage and frequency) for each of the four questions are shown in detail. The results are rounded up to one decimal place.

Q12. How many Facebook friends do you have?

		Frequency	Percent	Cumulative Percent
Valid	< 100	697	19,6	19,6
	100 - 199	1098	30,9	50,4
	200 - 299	806	22,7	73,1
	300 - 399	518	14,6	87,7
	400 - 499	225	6,3	94,0
	500 - 599	110	3,1	97,1
	> 600	104	2,9	100,0
	Total	3558	100,0	

Table 11: Results to Q12

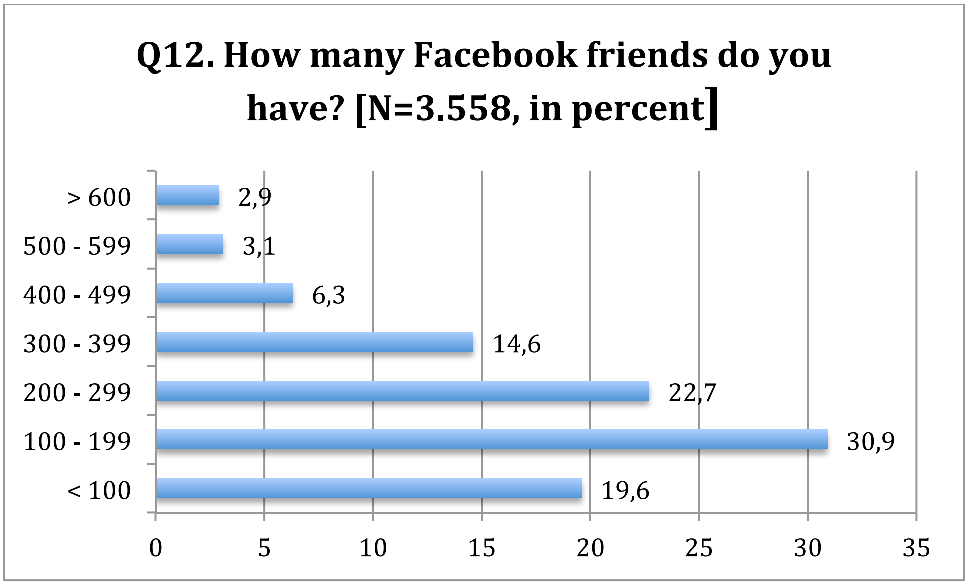


Figure 15: Results to Question 12

Q13_1. Are any co-workers among your Facebook friends?

		Frequency	Percent	Cumulative Percent
Valid	Yes	2762	77,6	77,6
	No	796	22,4	100,0
	Total	3558	100,0	

Table 12: Results to Question 13.1

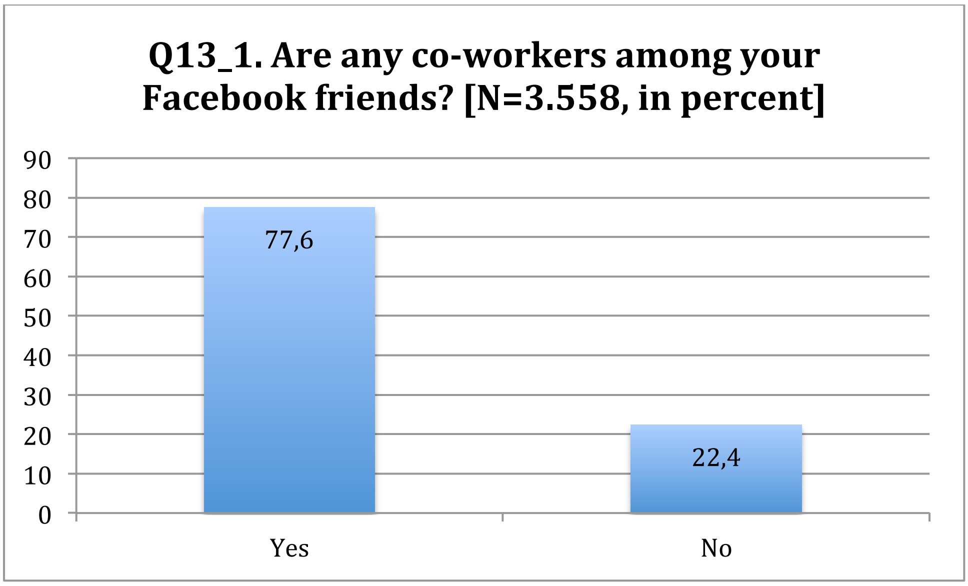


Figure 16: Results to Question 13.1

Q13_2. Are any superior/bosses among your Facebook friends?

		Frequency	Percent	Cumulative Percent
Valid	Yes	562	15,8	15,8
	No	2996	84,2	100,0
	Total	3558	100,0	

Table 13: Results to Question 13.2

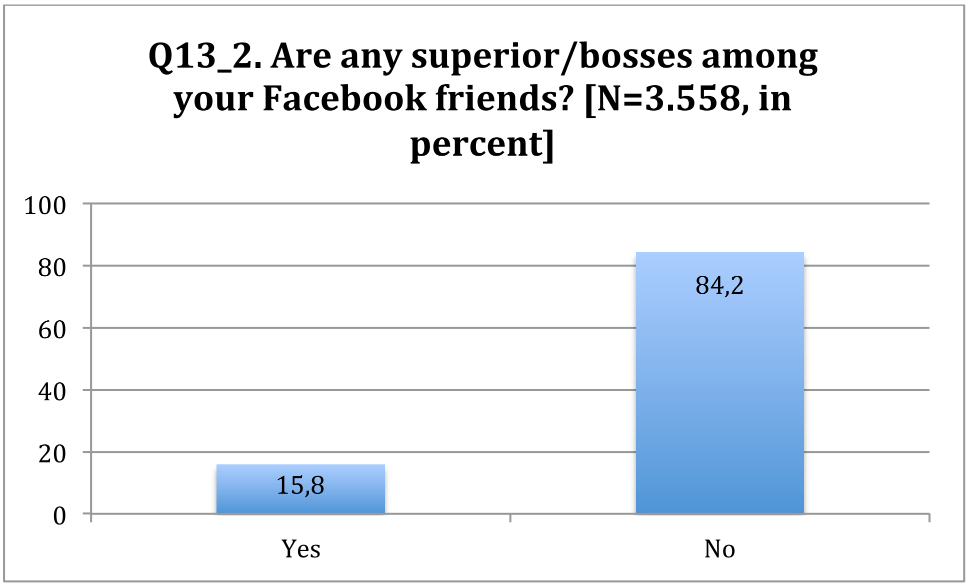


Figure 17: Results to Question 13.2

Q13_3. Are any Professors/Lecturers among your Facebook friends?

		Frequency	Percent	Cumulative Percent
Valid	Yes	464	13,0	13,0
	No	3094	87,0	100,0
	Total	3558	100,0	

Table 14: Results to Question 13.3

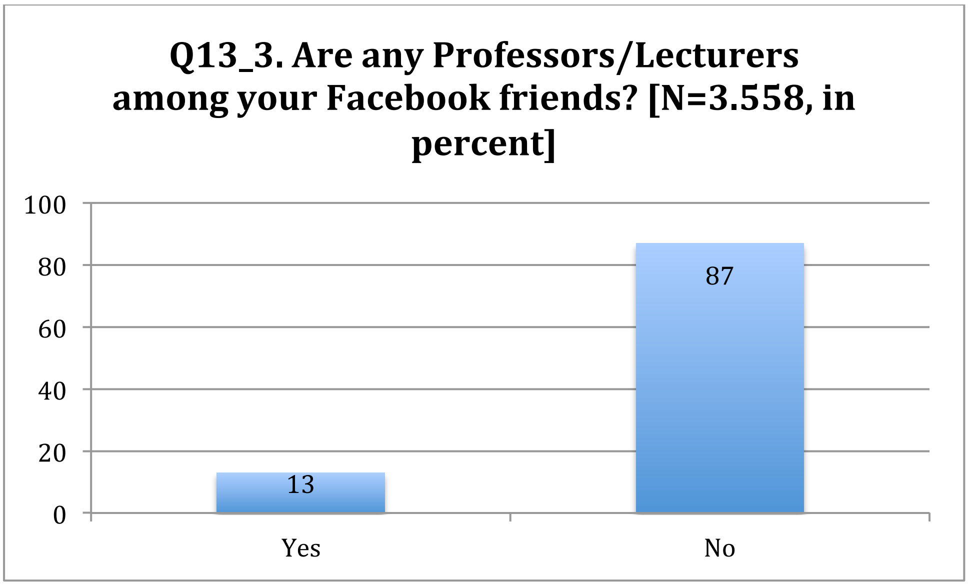


Figure 18: Results to Question 13.3

4.1.4 Privacy Settings

When evaluating our respondents' information behaviour we were especially interested in how they interact with and control their profiles' privacy settings. We therefore asked the respondents to tell us their general privacy settings for their Facebook profile. We provided them with detailed screenshots on where to find this setting, in case they didn't know. Surprisingly, only 3% of the study participants have chosen "public" as their general privacy setting. This means that almost all of our respondents care for their privacy and have changed Facebook's default privacy setting to a more private option. The majority (57.5%) makes their profile available only to friends, and 39.5% have further customized these settings. With Facebook's constant stream of changes, keeping up with one's privacy setting can be consuming. We therefore asked how many of the users try to keep up with the constant changes and adapt their settings accordingly. Quite a huge number of the respondents do change their default settings regularly. 42.4% checked that they have changed the setting three to eight times, 22.7% have changed them even more often than eight times. Nearly a third (30.2%) have at least changed them once or twice, and only 2.8% have never changed them. The remaining 1.9% can't recall if and how often they have changed the settings.

Next, we asked if and how closely users read the privacy policy and terms of service when they join or use a social networking site. Only 16.4% of the respondents answered that they read the policy "nearly completely" or "always in detail". The biggest part checked that they read the privacy policy and terms of use only "superficially/hardly ever" (38%) or only "partially" (34.2%). The remaining 11.4% even stated that they "never" read the privacy policy/terms of service. This finding further provides a basis for the claim stated by many scholars and civil rights activists that privacy policies often are lengthy, complicated and confusing (Fuchs, 2011c; Fernback and Papacharisi, 2007; Sandoval, 2010).

We also asked the study participants if they have ever blocked a Facebook Application (such as birthday calendar, FarmVille, Cities I've visited), because it accesses their data. Nearly three quarters of the respondents (74.6%) stated that they did so, 8.2% answered that though they have never blocked an application, they are worried that some applications access a lot of their data. 10.7% never activated or used a Facebook Application. Only 2.6% of our respondents are not bothered that Facebook Applications access a lot of data.

In the following, the results (percentage and frequency) for each of the four questions are shown in detail. The results are rounded up to one decimal place.

Q14. Which privacy settings have you chosen for Facebook?

		Frequency	Percent	Cumulative Percent
Valid	Public	107	3,0	3,0
	Friends	2046	57,5	60,5
	Custom	1405	39,5	100,0
	Total	3558	100,0	

Table 15: Results to Question 14

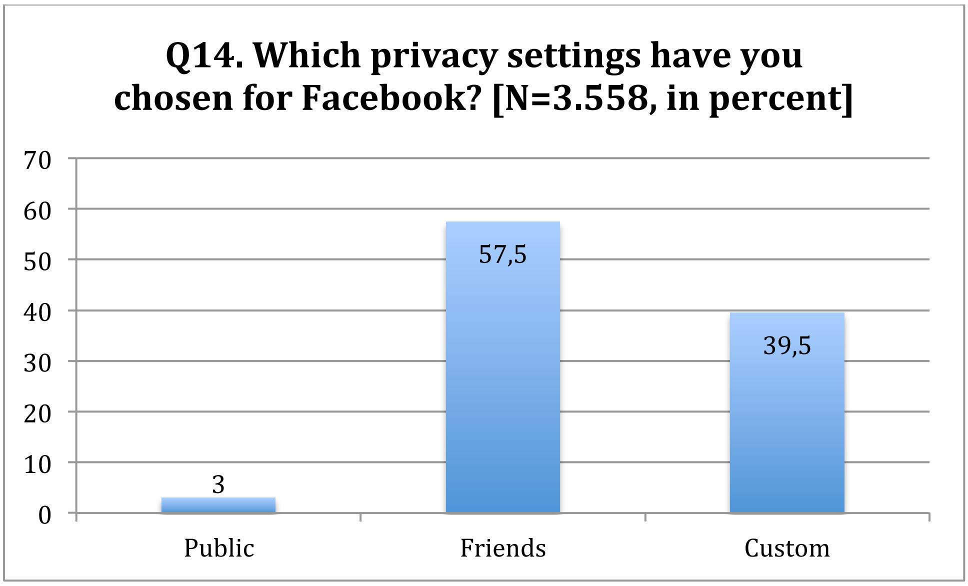


Figure 19: Results to Question 14

Q16: When you join or use a social networking site, do you read the privacy policy and terms of service?

		Frequency	Percent	Cumulative Percent
Valid	No, never	405	11,4	11,4
	Superficially/Hardly ever	1352	38,0	49,4
	Partially	1217	34,2	83,6
	Nearly completely	472	13,3	96,9
	Always in detail	112	3,1	100,0
	Total	3558	100,0	

Table 16: Results to Question 16

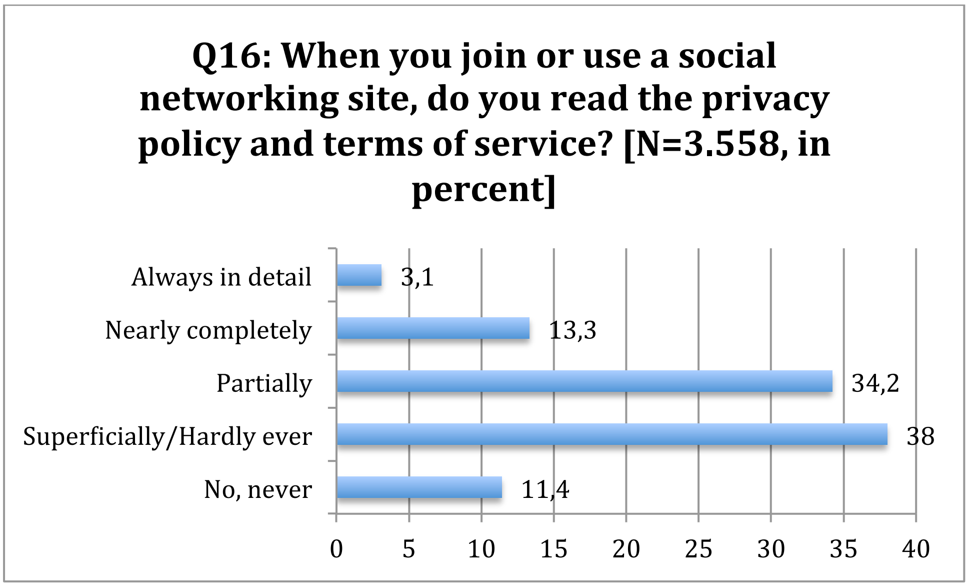


Figure 20: Results to Question 16

Q18: Have you ever changed the default privacy settings for Facebook? If yes, how often?

		Frequency	Percent	Cumulative Percent
Valid	No, never	100	2,8	2,8
	Yes, once or twice	1076	30,2	33,1
	Yes, three to eight times	1509	42,4	75,5
	Yes, more often than eight times	807	22,7	98,1
	I don’t know	66	1,9	100,0

		Frequency	Percent	Cumulative Percent
Valid	No, never	100	2,8	2,8
	Yes, once or twice	1076	30,2	33,1
	Yes, three to eight times	1509	42,4	75,5
	Yes, more often than eight times	807	22,7	98,1
	I don't know	66	1,9	100,0
	Total	3558	100,0	

Table 17: Results to Question 18

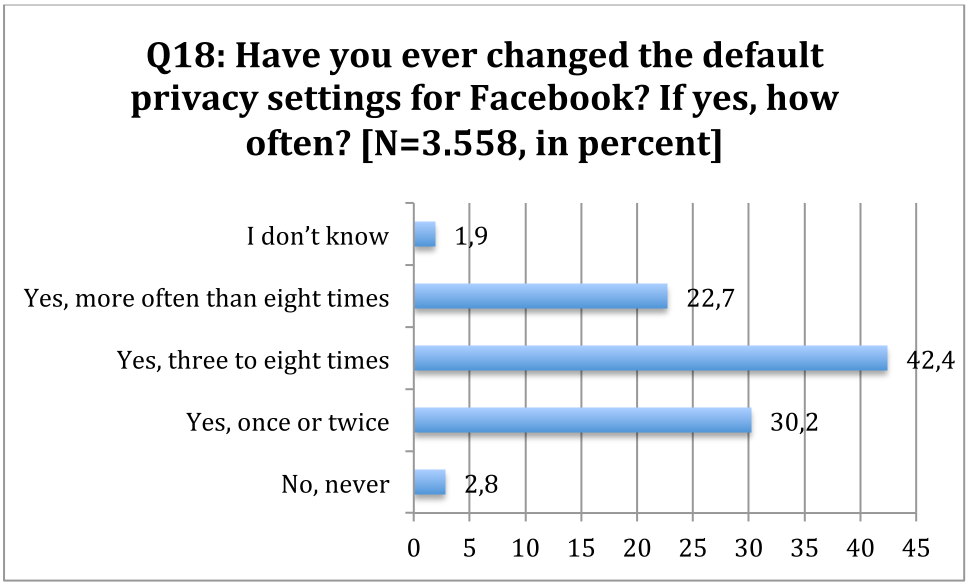


Figure 21: Results to Question 18

Q19. Have you ever blocked a Facebook Application (as e.g. birthday calendar, FarmVille, Cities I've visited…), because it accesses your data?

		Frequency	Percent	Cumulative Percent
Valid	Yes	2656	74,6	74,6
	No, that doesn't bother me	93	2,6	77,3
	No, but it worries me, when I see, that some applications access a lot of my data.	291	8,2	85,4
	I have never activated or used a Facebook Application	381	10,7	96,1
	I don't know	137	3,9	100,0
	Total	3558	100,0	

Table 18: Results to Question 19

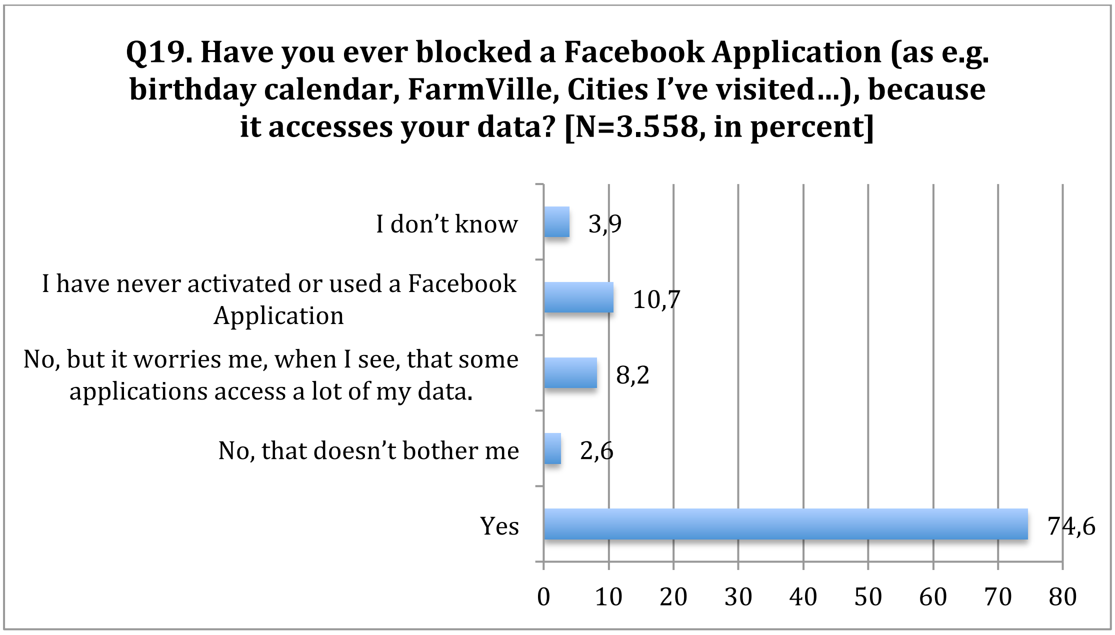


Figure 22: Results to Question 19

4.1.5 Advertising

When exploring the information behaviour of our study participants we also wanted to evaluate how they interact with advertisements and commercial sites/groups on Facebook and what kind of settings they have chosen for different forms of social media advertising that Facebook employs.

When we asked respondents if they have ever clicked on advertisements displayed on Facebook, 22% checked that they have done so. Asked if they have ever joined a group or site that has been established and is run by a commercial actor (e.g. local restaurants or shopping malls, brand communities such as Starbucks, Nike, etc.), a majority of 63.9% checked "yes" as an answer.

Facebook provides two settings that define how someone's profile can be used for advertising purposes. Users can choose whether or not friends can see which products or services one likes (Question 29) and they can define whether third parties are allowed to use a user's name or profile for advertising purposes (Question 28). We provided respondents with detailed screenshots in order to make it easier for them to look up these settings and give an accurate answer. Facebook offers two answering options "No one" and "only friends". By default the option "only friends" is activated. For question 28 52.7% of our respondents have changed this setting to "no one", for question 29 nearly similar 53.8% have changed the setting to "no one".

More findings on advertising on Facebook, and users knowledge, attitudes and concerns can be found in the section on "Targeted Advertising".

In the following, the results (percentage and frequency) for each of the four questions are shown in detail. The results are rounded up to one decimal place.

Q23. Have you ever clicked on an advertisement displayed on Facebook?

		Frequency	Percent	Cumulated Percent
Valid	Yes	783	22,0	22,0
	No	2571	72,3	94,3
	I don't know	204	5,7	100,0
	Total	3558	100,0	

Table 19: Results to Question 23

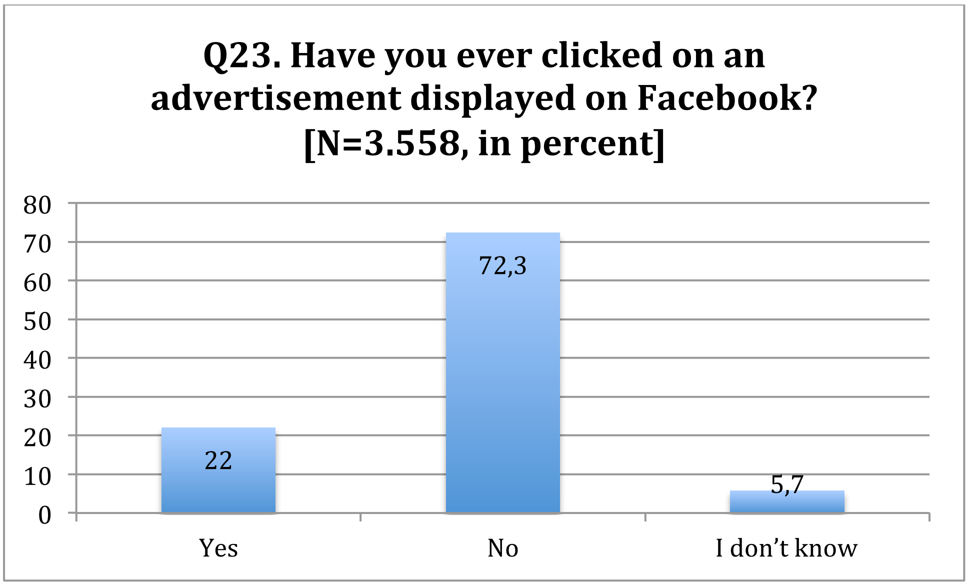


Figure 23: Results to Question 23

Q28. What is your setting that defines whether third parties are allowed to use your name or profile for advertising purposes?

		Frequency	Percent	Cumulated Percent
Valid	No one	1874	52,7	52,7
	Only friends	1684	47,3	100,0
	Total	3558	100,0	

Table 20: Results to Question 28

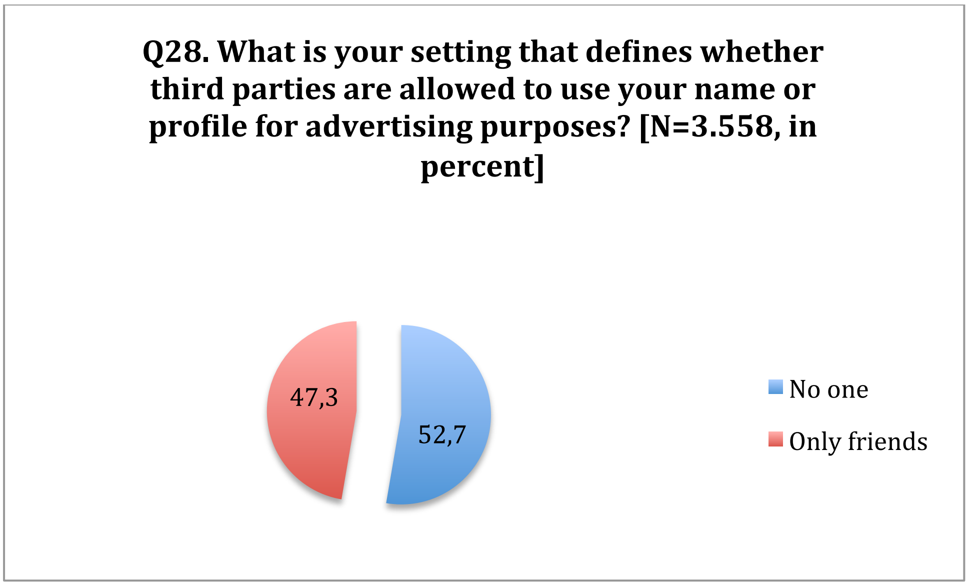


Figure 24: Results to Question 28

Q29. What is your setting, that defines whether friends can see which products or services you like?

		Frequency	Percent	Cumulated Percent
Valid	No one	1914	53,8	53,8
	Only friends	1644	46,2	100,0
	Total	3558	100,0	

Table 21: Results to Question 29

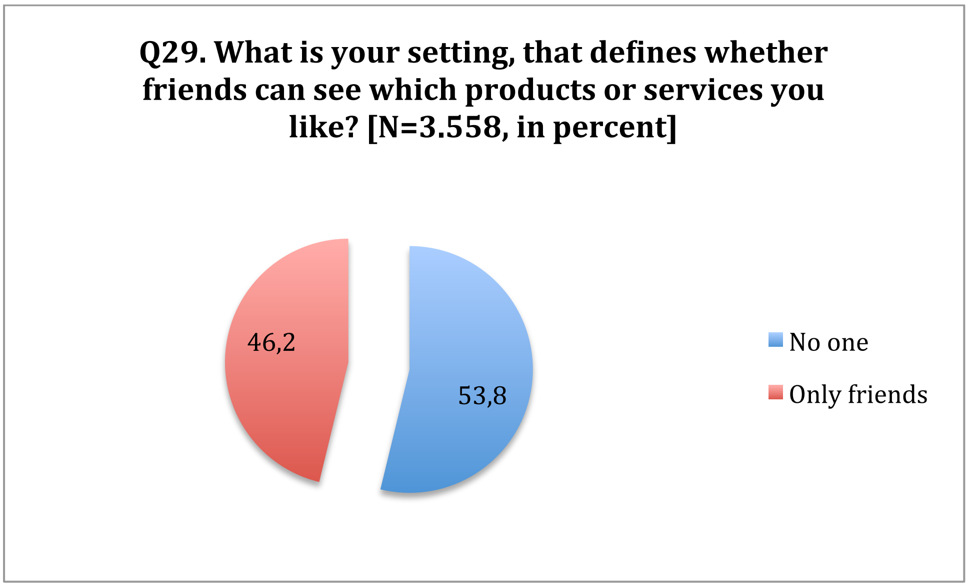


Figure 25: Results to Question 29

Q26. Have you ever joined a group or site that has been established and is run by a commercial actor (e.g. local restaurants or shopping malls, brand communities such as Starbucks, Nike, etc.)?

		Frequency	Percent	Cumulated Percent
Valid	Yes	2272	63,9	63,9
	No	1126	31,6	95,5
	I don't know	160	4,5	100,0
	Total	3558	100,0	

Table 22: Results to Question 26

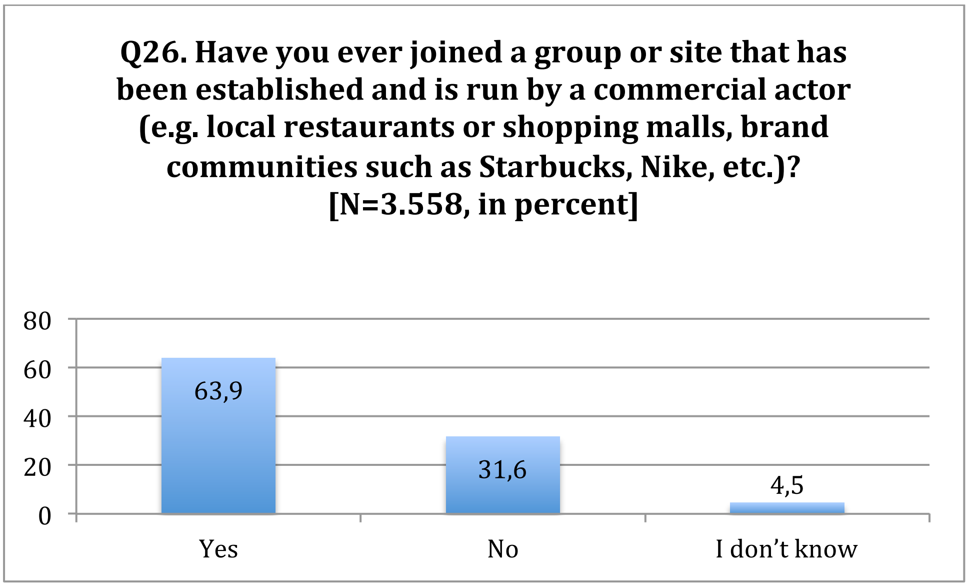


Figure 26: Results to Question 26

4.1.6 Information Behaviour Index

Our aim was to build an index from all these questions, which evaluates the information behaviour of our respondents and allows us to correlate this behaviour with other variables such as surveillance knowledge, surveillance attitude, or privacy concern. Therefore we analysed all the items and identified two different types of questions: the first category are questions that explore the dimension of the intensity of the information behaviour, the second category assessed the carefulness of such information behaviour.

Accordingly we were able to build two indices:

a) Carefulness Index
b) Intensity Index

For both indices we chose the suitable items from the comprehensive list of 21 questions above by running a correlation analysis, in order to obtain reliable indices. We calculated Cronbach's Alpha coefficient, which measures how well a set of items measures a single uni-dimensional latent construct. Based on the coefficient, decisions can be made regarding the addition, subtraction or modification of items. Alpha is expressed as a number between 0 and 1. The value of alpha is influenced by the amount of questions, the interrelatedness between items and the homogeneity of a construct. However, a high coefficient alpha does not always mean a high degree of internal consistency. This is because the length of a measurement (i.e. number of itmes) also affects alpha. If the length is too short, the value of alpha is reduced. Typically a value above 0.7 is considered acceptable. For short instruments (5-10 items), the suggestion is that an Alpha value of at least 0.5 should be achieved. (Cronbach 1951, Kehoe 1995, Helmstater 1964, Nunnally 1978)

a) Carefulness of Information Behaviour Index

In order to assess hypotheses 8-11 it is necessary to measure and evaluate "careful information behaviour" on social networking sites, which is influenced by e.g. the degree of activation of privacy mechanisms, or the degree of deactivation of advertising options.

From the list of all questions concerning information behaviour we identified the following six items to reliably test for the carefulness of respondents' information behaviour:

1. Which privacy settings have you chosen for Facebook?
2. Have you ever changed the default privacy settings for Facebook? If yes, how often?
3. (When Facebook changes its privacy policy or terms of service without user notification, regularly some users via their status updates spread these changes.) Have you yourself ever participated in informing other users about changes in the privacy policy or terms of service?
4. Have you ever blocked a Facebook Application (as e.g. birthday calendar, FarmVille, Cities I've visited…), because it accesses your data?
5. What is your setting that defines whether third parties are allowed to use your name or profile for advertising purposes?
6. What is your setting, that defines whether friends can see which products or services you like?

For an index comprising these six items we received a Cronbach Alpha of 0.63, which is acceptable for such a short measurement. In order to calculate the index we recoded the answers to the questions (with the value "1" always coding the least careful answering option). Since the scaling of the answering options was different, with some questions offering only 2 answers (e.g. value 1 and 2) and others offering 4 answering options (e.g. values 1-4) we weighted the values in order to adjust the highest possible values for all the questions. Then we added the values together and received results on a 27points scale. We split this range into four equal categories labelled "very careless", "careless", "careful", "very careful". The results are illustrated in the table and figures beyond, showing that 28% of the respondents have a very careful information behaviour, and 30.8% have a careful information behaviour when it comes to social networking sites. However, 29.8% of the respondents still show careless information behaviour, and yet 11.4% act very careless about their informational privacy on social networking sites.

Carefulness Index

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Careless	406	11,4	11,4	11,4
Careless	1060	29,8	29,8	41,2
Careful	1095	30,8	30,8	72,0
Very Careful	997	28,0	28,0	100,0
Total	3558	100,0	100,0	

Table 23: Distribution Carefulness of Information Behaviour Index

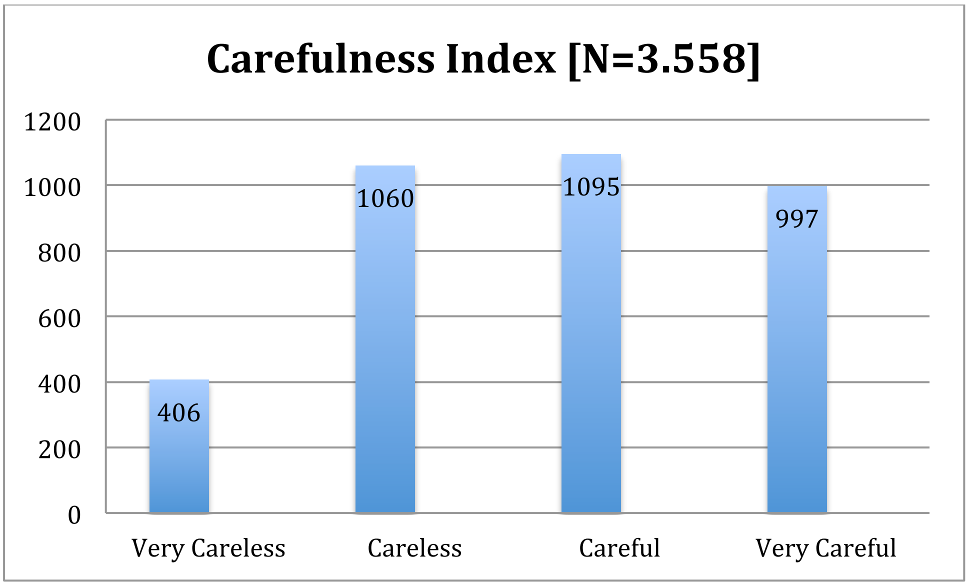


Figure 27: Distribution Carefulness of Information Behaviour (Frequency)

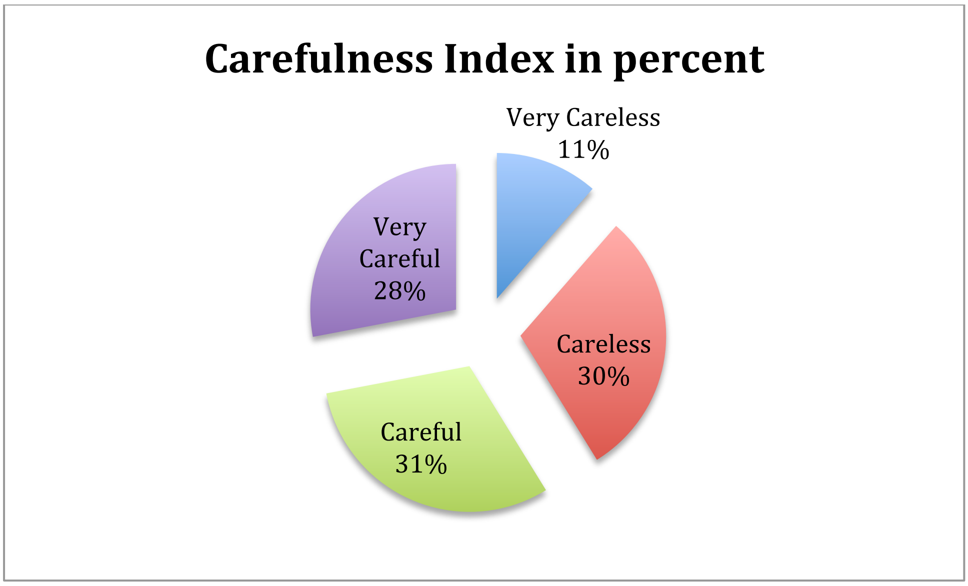


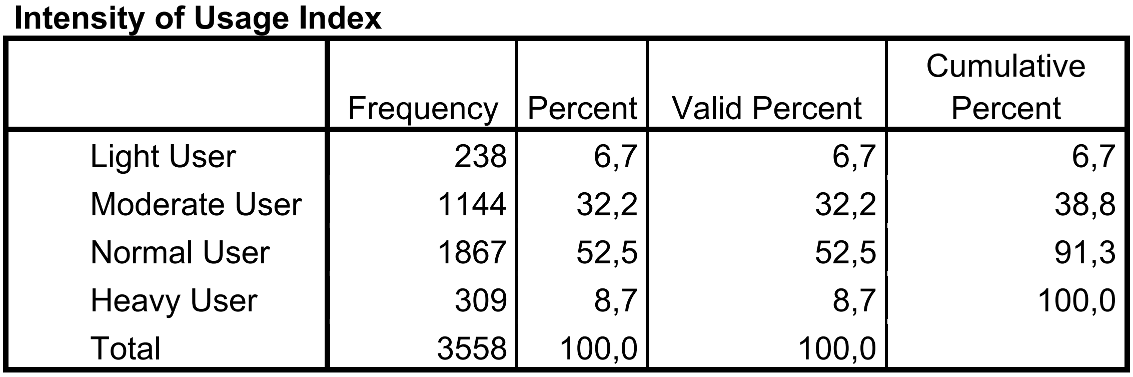
Figure 28: Distribution Carefulness of Information Behaviour (Percentage)

b) Intensity of Usage Index

Additionally to the degree of careful information behaviour, the items we measured in order to evaluate information behaviour allowed us to calculate the intensity of usage behaviour, i.e. how heavy someone uses social networking sites. From the list of all questions concerning information behaviour we identified the following nine items to test for the intensity of respondents' information behaviour:

1. How often do you use Facebook?
2. How often do you upload pictures to social networking sites, in order to share them with others?
3. How often do you upload videos to social networking sites, in order to share them with others?
4. How often do you share a comment or status on social networking sites?
5. How often do you write messages or chat with other users on social networking sites?
6. How many Facebook friends do you have?

We tested internal reliability by using the standardised Cronbach alpha coefficient and received a good result of 0.76. We recoded and weighted the answers in order to obtain a suitable measurement. The resulting range of answers was divided into the four categories of "heavy user", "normal user", "moderate user", and "light user". The index shows that 8.7% of the respondents fall in the category of heavy users, tending to use Facebook several times a day in a very active manner (uploading pictures, commenting and posting status updates, chatting with other users, and so on). The 52.5% of “normal users” do use Facebook regularly, usually several times a week, often also on a daily basis but do not engage as actively as the heavy users. 32.2% show moderate usage intensity, checking in on Facebook several times a week, rarely updating their profiles with comments, pictures, and videos. Light users, which make up 6.7% of our sample, typically log in on Facebook less than once a month and use it overall in a passive manner, tending not to engage in activities such as uploading content or interacting with other users.



Intensity of Usage Index

	Frequency	Percent	Valid Percent	Cumulative Percent
Light User	238	6,7	6,7	6,7
Moderate User	1144	32,2	32,2	38,8
Normal User	1867	52,5	52,5	91,3
Heavy User	309	8,7	8,7	100,0
Total	3558	100,0	100,0	

Table 24: Distribution Intensity of Usage Index

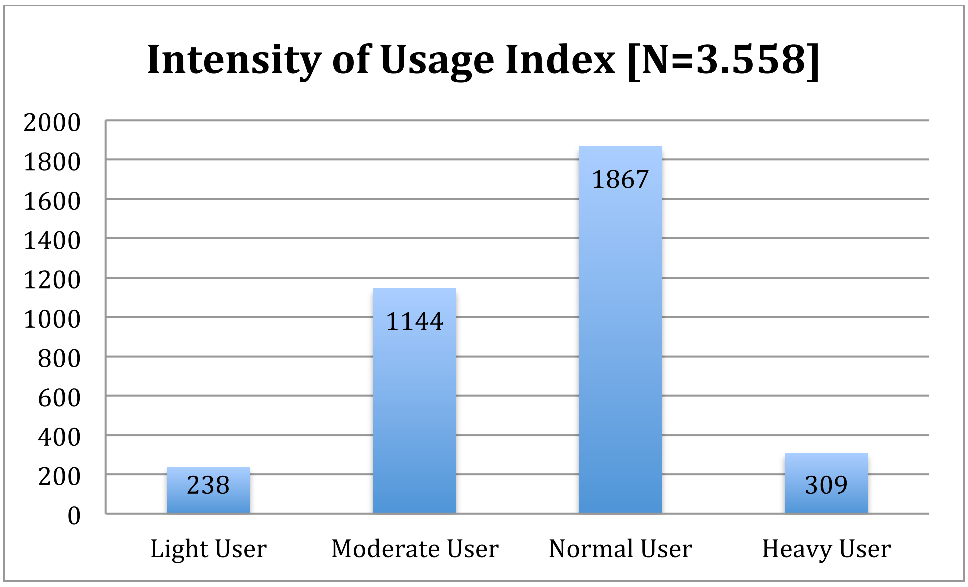


Figure 29: Distribution Intensity of Usage Index (Frequency)

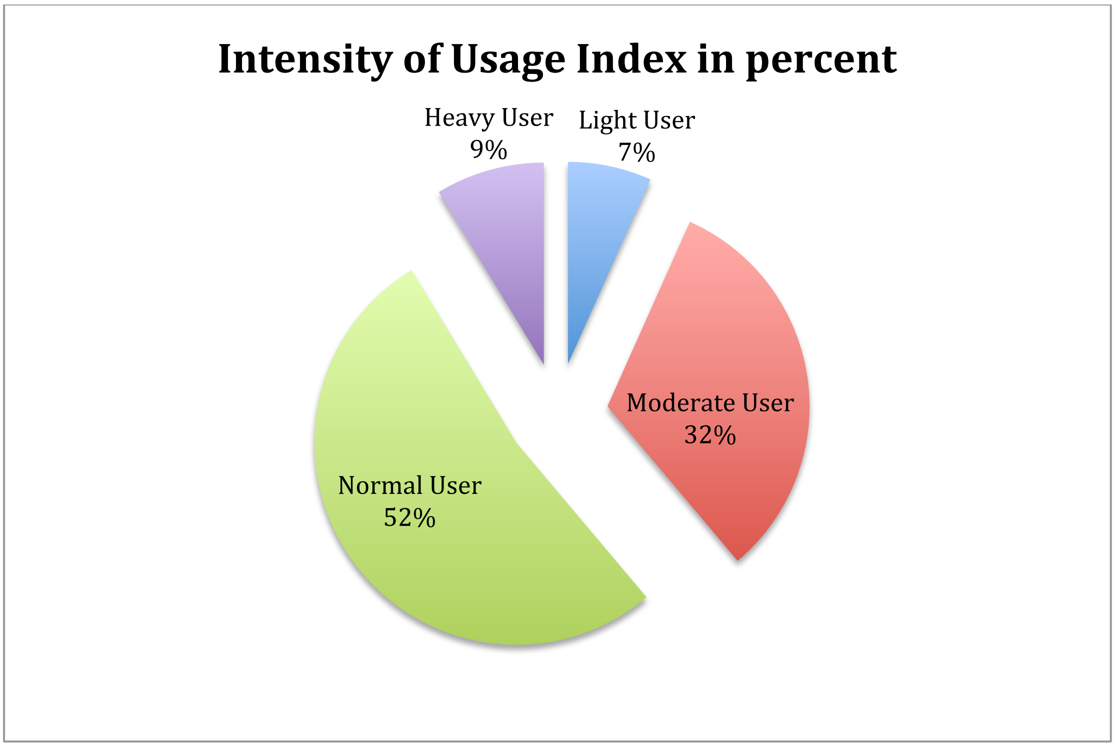


Figure 30: Distribution Intensity of Usage Index (Percentage)

4.1.7 Correlations

A Spearman's Rank Order correlation was run to determine the relationship between the degree of carefulness of respondents' information behaviour and the intensity of their usage. Additionally we ran correlational analysis with some demographic variables such as gender, age, average monthly income, respondents' parents' occupational and educational background.

Interestingly correlation between the Carefulness Index and the Intensity Index showed significantly positive results. A Spearman's rho of 0.167 indicates that the more intensively and actively respondents use Facebook, the more careful they are. A reason might be that heavy users have more experience in the usage of Facebook accordingly. They might be better informed about changes to privacy and advertising settings (since these are often spread via Facebook users themselves), and have invested more time in finding their way through complicated and sometimes well hidden settings. Additionally they might feel more vulnerable to privacy infringement since they upload and share a lot of data with their friends and therefore are more active in taking steps to protect their data.

Careful Information Behavior * Intensity of Usage Correlations

	Intensity Index	Carefulness Index

Intensity Index	Correlation Coefficient (Spearman’s Rho)	1,000	,167**
	Sig. (2-tailed)	.	,000
	N	3558	3558
Carefulness Index	Correlation Coefficient (Spearman’s Rho)	,167**	1,000
	Sig. (2-tailed)	,000	.
	N	3558	3558

**. Correlation is significant at the 0.01 level (2-tailed).

Table 25: Correlation Careful Information Behaviour with Intensity of Usage

Correlation analysis of the two indices with some demographic variables showed two interesting findings. We found that the Intensity Index was significantly correlated with age, and to a lesser degree to the average monthly income, indicating that older study participants show lighter usage behaviour than younger participants. Respondents with a lower average income may also tend to use Facebook less intensively. This might be du to a lesser amount of spare time, since they probably have to work additionally to their studies. The second interesting finding is a – though rather weak – significantly positive correlation between the degree of carefulness and age, suggesting that older respondents tend to be slightly more careful.

Correlations

		Intensity Index	Carefulness Index
Age	Correlation Coefficient (Spearman’s Rho)	-,225**	,050**
	Sig. (2-tailed)	,000	,003
	N	3558	3558
Average Monthly Income	Correlation Coefficient (Spearman’s Rho)	-,080**	,030
	Sig. (2-tailed)	,000	,075
	N	3553	3553

**. Correlation is significant at the 0.01 level (2-tailed).

Table 26: Correlation Intensity of Usage with demographic variables

Hypothesis 8: More knowledge about surveillance is significantly positively correlated to more careful information behaviour on SNS (intensity of reading the terms of use, degree of deactivation of advertising options, degree of activation of privacy mechanisms).

In order to assess this hypothesis it is necessary to clarify what "knowledge about surveillance" means and how it can be operationalized:

4.2 Variable #2: Surveillance Knowledge

In context of our study we can differentiate knowledge about surveillance along two main lines:

- (1) who surveils – actor of surveillance
  - individuals
  - political actors (nation-states, executive forces, military,…)
  - economic actors (companies, superiors,..)

- (2) where does surveillance take place – fields of surveillance
  - surveillance in general/offline
  - surveillance online
  - surveillance on social networking sites

Since we are especially interested in the economic dimension of surveillance on social networking sites, the focus will be on the combination of 1.3 and 2.3 i.e. surveillance on social networking sites by economic actors. However in order to fully assess students knowledge about surveillance we also asked questions concerning surveillance in general, e.g. testing their knowledge about what rules and legislations in Austria apply to privacy and data protection.

Existing studies suggest that knowledge about economic surveillance is low (Fuchs 2009; Turow, Feldman, and Meltzer 2005; Turow, Hennessy, and Bleakley 2008; Zureik, Stalker, and Smith 2010; Phelps, Nowak, and Ferrell 2000). Some studies (Chan, Harling Stalker, and Lyon 2010; Milne and Rohm 2000) aimed at measuring participant's self-assessment of surveillance and privacy knowledge. However, we suppose that self-assessment of knowledge will lead to distorted or false results due to wrongful (consciously and unconsciously) answers. Therefore we will test factual knowledge in order to achieve reliable results.

Several studies found that knowledge about surveillance on social networking sites, on the one hand, and privacy settings and opportunities, on the other hand, is similarly low (Chan, Harling Stalker, and Lyon 2010; Milne and Rohm 2000). Acquisti and Gross (2006, 53) found that many users "mistakenly believe that FB does not collect information about them from other sources regardless of their use of the site (67%), that FB does not combine information about them collected from other sources (70%), or that FB does not share personal information with third parties (56%)." These findings suggest that users have a low level of knowledge about surveillance on Facebook. In the same survey, Acquisti and Gross (2006, 52–53), found that "almost 77% of respondents claimed not to have read FB's privacy policy (the real number is probably higher)" and that a significant minority (around 25%) are not aware of tools and options Facebook offers in its complex privacy and account settings. These additional findings suggest that many users not only do not know much about surveillance on social networking sites, but that they also tend to be careless in their information behaviour.

Though Debatin et al. (2009, 93) show a different image of users' knowledge and information behaviour (i.e. that of well informed and careful users), they found that "the vast majority of Facebook users (91%) claimed indeed to be familiar with Facebook privacy issues and were also likely to restrict their profiles (77%) through privacy settings", thereby indicating a correlation between knowledge and behaviour.

Accordingly we hypothesize that more knowledge about surveillance is significantly positively correlated to more careful information behaviour on social networking sites.

In the questionnaire, we evaluated surveillance knowledge by asking questions about concrete surveillance topics such as Facebook's right to sell personal data to third parties, Facebook's new advertising feature "social ads", the European Data Retention Directive, the Austrian Data Protection Law.

We conceptualized variable #2 Surveillance Knowledge by posing respondents a set of eight questions, that test their knowledge about surveillance in general as well as in context of social networking sites.

- Business organizations excessively collect and store personal information about customers.
- When a Website has a privacy policy, it means the site will not share my information with other Websites or companies
- In Austria the Data Retention Directive by the European Union has already been implemented
- Websites registered in Austria have to pass on personal data (e.g. name, email-address, location data, IP-address, information about whom and when you've sent a message or which profiles you've looked at] to the police upon request.]
- Facebook is allowed to give my personal data (e.g. contact information, interests, activities, friends, online behaviour) to third parties/other companies for advertising purposes.
- Advertisements, commercial sites and paid services on social networking sites, like Facebook, must be marked as such.
- On Facebook all users see the same advertisements.

- In Austria companies are allowed to electronically surveil their employees (e.g. monitor and analyse which websites an employee visits, which emails an employee sends or register every keystroke).

Respondents were asked if the presented statement was true or false. Also, an "I don't know"-answering category was provided.

For only three out of the eight questions a majority of the respondents knew the right answer: For Question 35 "Business organizations excessively collect and store personal information about customers" 92% answered "yes, that's true", which is the correct answer. Not quite as much, but still more than half of the respondents (62.6%) chose the right answer for Question 36 "When a Website has a privacy policy, it means that the site will not share my information with other Websites or companies". Additionally a clear majority of 83.2% was aware that the statement "On Facebook all users see the same advertisements" (Q41) is false.

Asked about the Data Retention Directive ("In Austria the Data Retention Directive by the European Union has already been implemented") the majority of the respondents answered that they don't know the answer (59.8%), 21.1% gave the wrong answer (Yes, that's true), and only 19.1% knew the correct answer (No, that's false).

For four questions the majority of the respondents checked the wrong answer.

Only 6.7% knew the correct answer to question 38 "Websites registered in Austria have to pass on personal data (e.g. name, email-address, location data, IP-address, information about whom and when you've sent a message or which profiles you've looked at] to the police upon request". Also, asked if in Austria companies are allowed to electronically surveil their employees (e.g. monitor and analyse which websites an employee visits, which emails an employee sends or register every keystroke) (Q42), only 20.2% chose the right answer.

When asked, if it is true that Facebook is allowed to give personal data (e.g. contact information, interests, activities, friends, online behaviour) to third parties/other companies for advertising purposes, respondents were not sure about their answers. 31.8% checked "I don't know", another third (32.6%) thought it was correct (which is actually the right answer), and a very small majority of 35.6% answered with " No, that's false".

Huge uncertainty also determined the answers to the question if advertisements, commercial sites and paid services on social networking sites, such as Facebook, must be marked as such. Only 19.4% knew the correct answer (No, that's false), 46.5% gave the wrong answer, and 34.1% of the respondents said that they don't know the answer. The following table shows the mean, standard error of mean and standard deviation for each question. Maximum is 10 (since for each correct answer 10 is the value), Minimum is 1 (which is the value for each wrong answer). "I don't know" – answers were assigned 0. We've chosen these values in order to account in our Surveillance Knowledge Index not only for the ratio between right and wrong answers (and "I don't know"), but also to easily identify and differentiate between those who scored specifically high on correct or incorrect answers (for further detail please see the section on the "Surveillance Knowledge Index" below).

	N (Valid)	Mean	Standard Error of Mean	Standard Deviation
Question 35	3558	9,226	0,0442	2,63645
Question 36	3558	6,4413	0,07745	4,61955
Question 37	3558	2,1197	0,06451	3,84786
Question 38	3558	1,3401	0,03955	2,35925
Question 39	3558	3,6166	0,07476	4,4592
Question 40	3558	2,4039	0,06291	3,75271
Question 41	3558	8,3449	0,06179	3,68586
Question 42	3558	2,5343	0,06346	3,78526

Table 27: Results to Questions 35-42

In the next table Mean, Minimum, Maximum and Standard Deviation for the amount of right answers, wrong answers, as well as I don't know answers are displayed. The table shows that on average respondents knew the right answer to 3.35 questions checked "I don't know" for 2.2 questions and answered wrongfully to 2.43 questions.

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Right Answer	3558	,00	8,00	3,3589	1,34437
Wrong Anwer	3558	,00	7,00	2,4376	1,34049
I don't know	3558	,00	8,00	2,2035	1,71522
Valid N (listwise)	3558				

Table 28: Minimum, Maximum, Mean, and Standard Deviation for Answering Categories

In the following, the results (percentage and frequency) for each of the eight questions are shown in detail. The results are rounded up to one decimal place. The correct answer is marked as such.

Q35: Business organizations excessively collect and store personal information about customers

		Frequency	Percent	Cumulative Percent
Valid	Yes, that's true. (right answer)	3275	92,0	92,0
	No, that's false.	76	2,1	94,2
	I don't know.	207	5,8	100,0

Total	3558	100,0	

Table 29: Results to Question 35

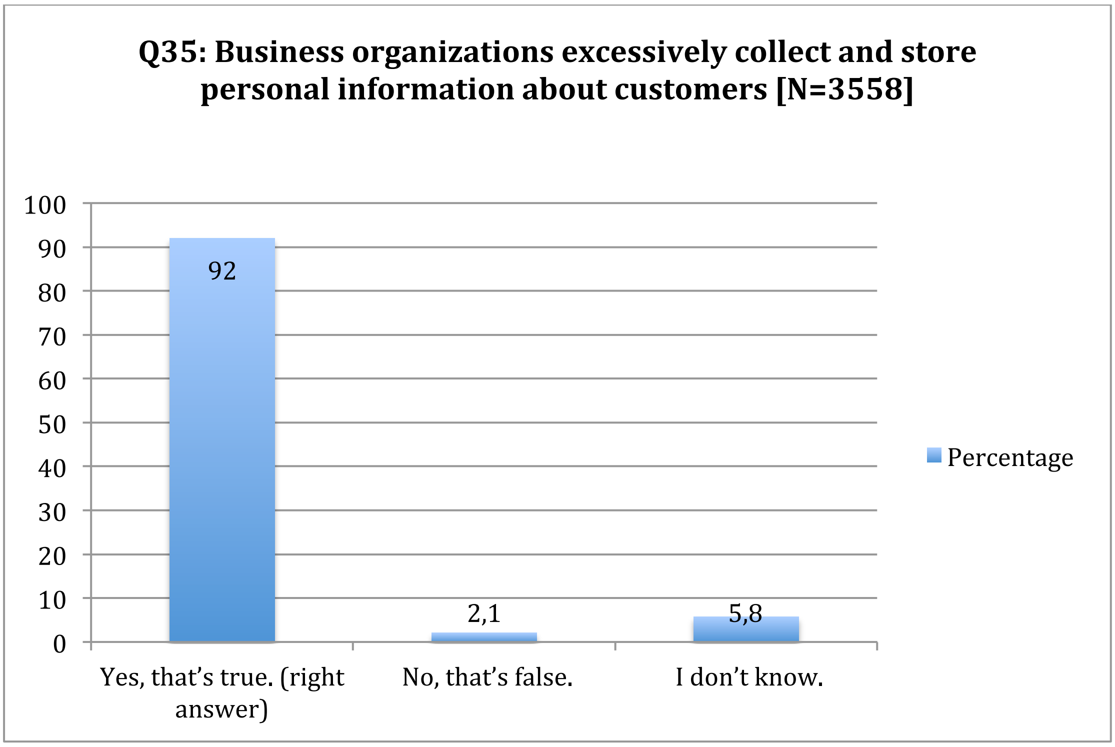


Figure 31: Results to Question 35

Q36: When a Website has a privacy policy, it means that the site will not share my information with other Websites or companies.

		Frequency	Percent	Cumulative Percent
Valid	Yes, that's true.	628	17,7	17,7
	No, that's false. (right answer)	2229	62,6	80,3
	I don't know.	701	19,7	100,0
	Total	3558	100,0	

Table 30: Results to Question 36

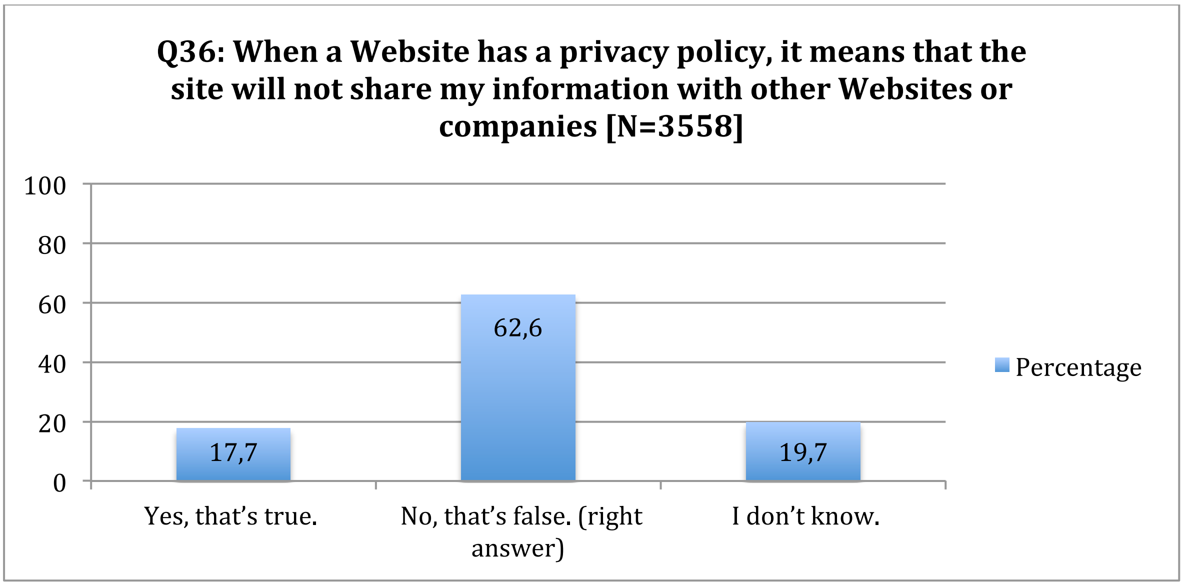


Figure 32: Results to Question 36

Q37: In Austria the Data Retention Directive by the European Union has already been implemented

		Frequency	Percent	Cumulative Percent
Valid	Yes, that's true.	752	21,1	21,1
	No, that's false. (right answer)	679	19,1	40,2
	I don't know.	2127	59,8	100,0
	Total	3558	100,0	

Table 31: Results to Question 37

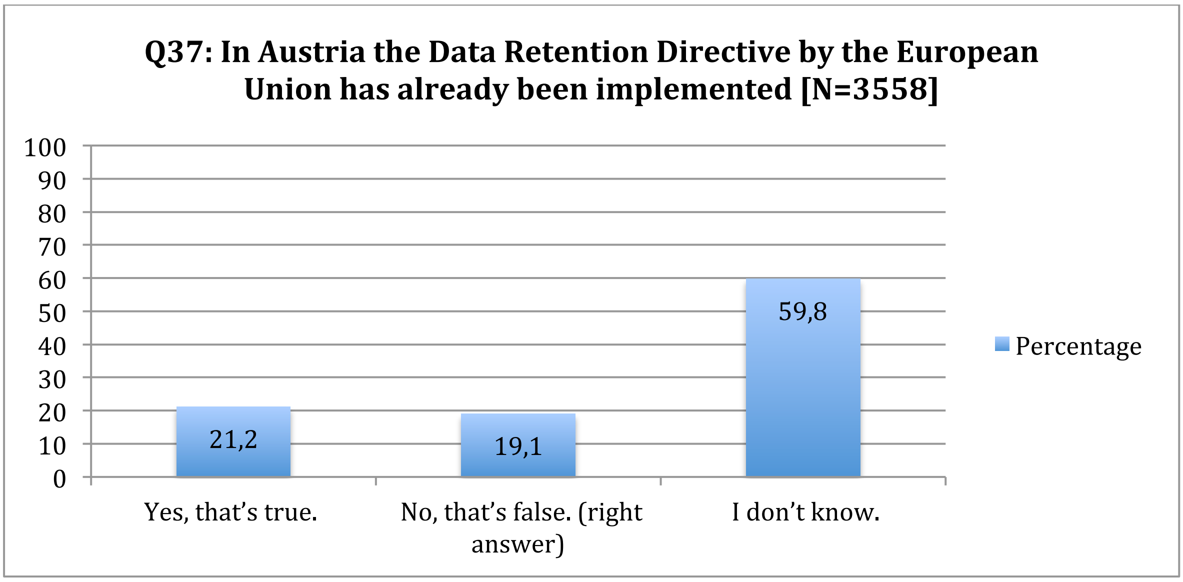


Figure 33: Results to Question 37

Q38: Websites registered in Austria have to pass on personal data (e.g. name, email-address, location data, IP-address, information about whom and when you've sent a message or which profiles you've looked at] to the police upon request.

		Frequency	Percent	Cumulative Percent
Valid	Yes, always if the police demand it. (right answer)	238	6,7	6,7
	No, never.	95	2,7	9,4
	Only if the police have a juridical order that was passed by a court and is handed over to the provider.	2293	64,4	73,8
	I don't know.	932	26,2	100,0
	Total	3558	100,0	

Table 32: Results to Question 38

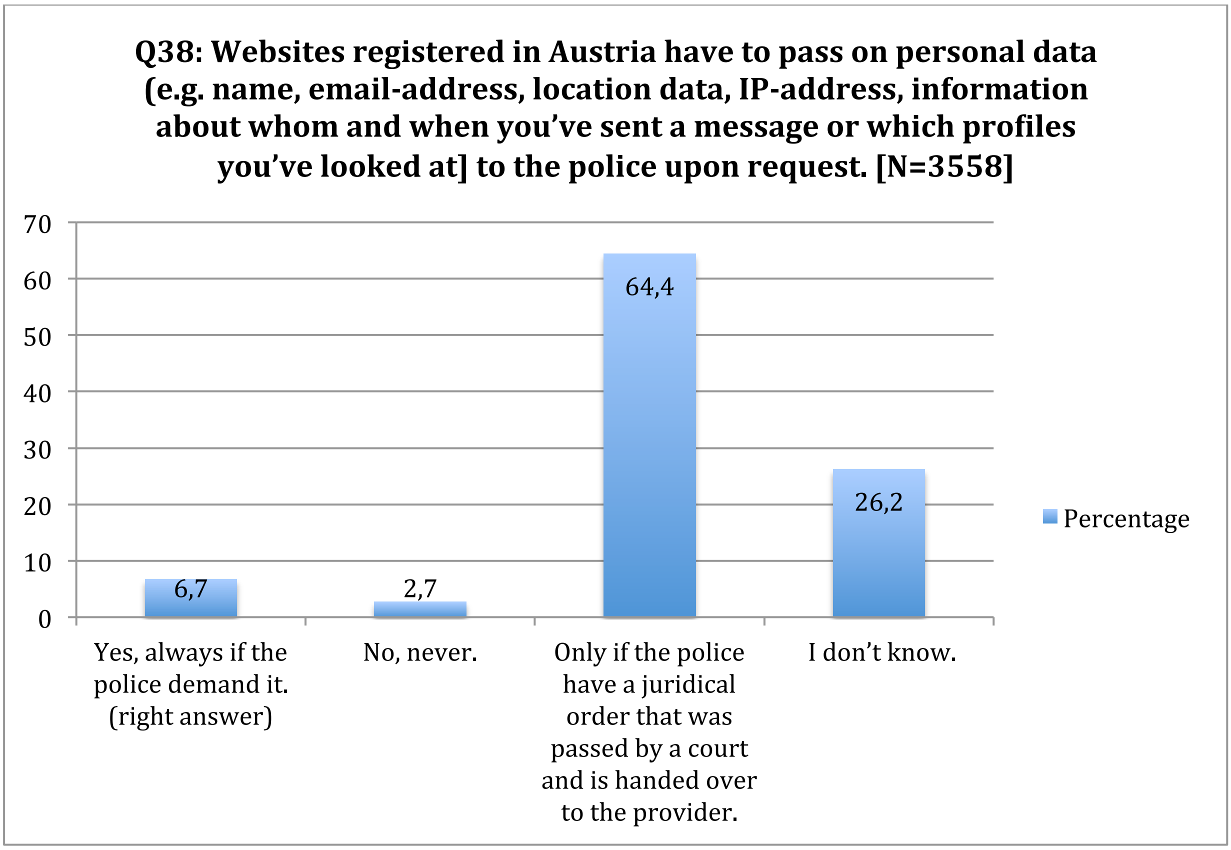


Figure 34: Results to Question 38

Q39: Facebook is allowed to give my personal data (e.g. contact information, interests, activities, friends, online behaviour) to third parties/other companies for advertising purposes.

		Frequency	Percent	Cumulative Percent
Valid	Yes, that's true. (right answer)	1160	32,6	32,6
	No, that's false.	1268	35,6	68,2
	I don't know.	1130	31,8	100,0
	Total	3558	100,0	

Table 33: Results to Question 39

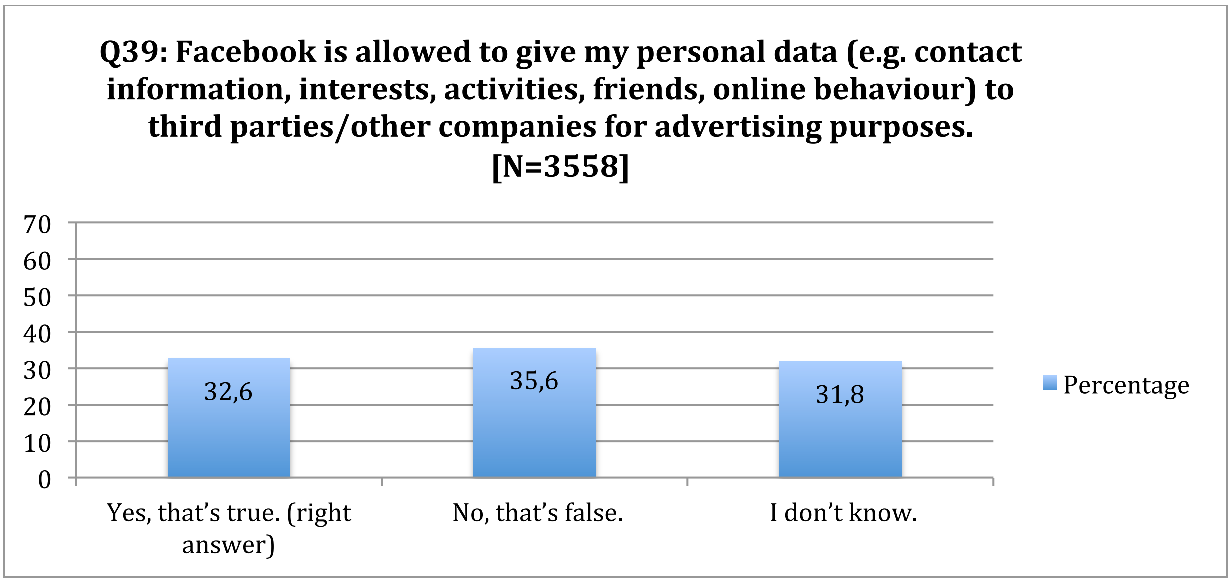


Figure 35: Results to Question 39

Q40: Advertisements, commercial sites and paid services on social networking sites, such as Facebook, must be marked as such.

		Frequency	Percent	Cumulative Percent
Valid	Yes, that's true.	1653	46,5	46,5
	No, that's false. (right answer)	690	19,4	65,9
	I don't know.	1215	34,1	100,0
	Total	3558	100,0	

Table 34: Results to Question 40

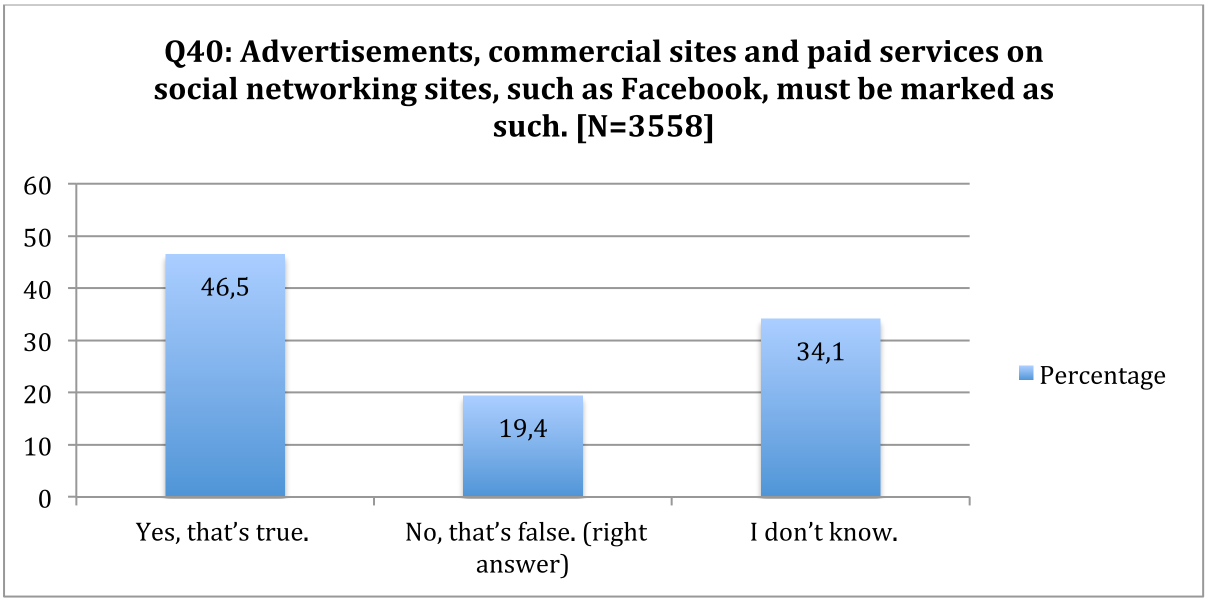


Figure 36: Results to Question 40

Q41: On Facebook all users see the same advertisements.

		Frequency	Percent	Cumulative Percent
Valid	Yes, that's true.	91	2,6	2,6
	No, that's false. (right answer)	2960	83,2	85,8
	I don't know.	507	14,2	100,0
	Total	3558	100,0	

Table 35: Results to Question 41

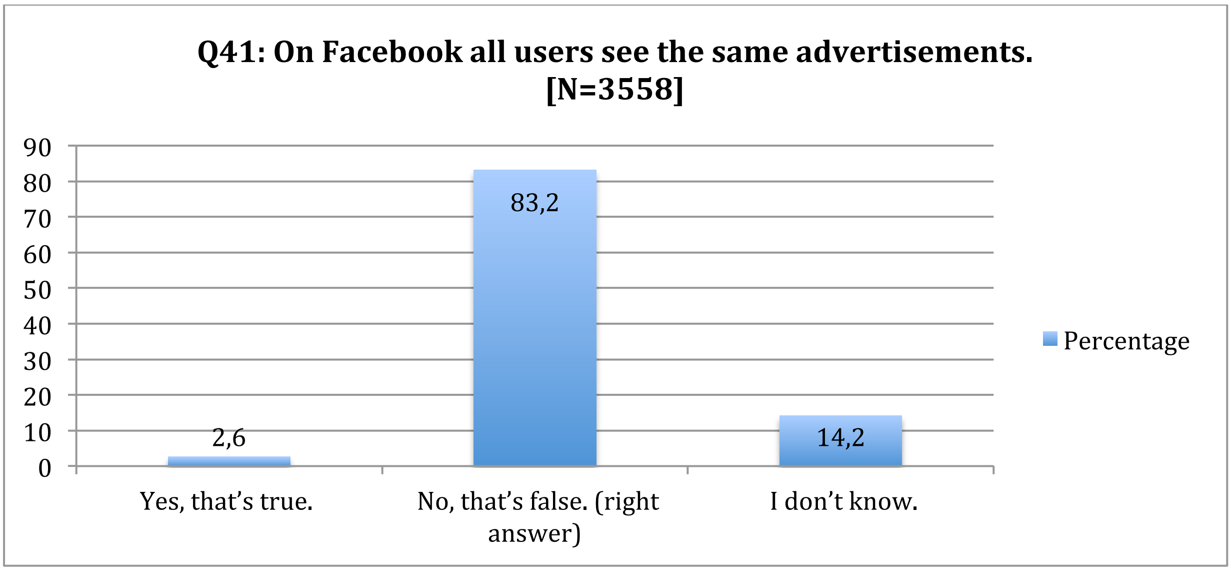


Figure 37: Results to Question 41

Q42: In Austria companies are allowed to electronically surveil their employees (e.g. monitor and analyse which websites an employee visits, which emails an employee sends or register every keystroke).

		Frequency	Percent	Cumulative Percent
Valid	Yes that's true. Companies are allowed to monitor their employees. (right answer)	720	20,2	20,2
	No, that's false. In any case, workplace surveillance is prohibited in Austria.	1817	51,1	71,3
	I don't know.	1021	28,7	100,0
	Total	3558	100,0	

Table 36: Results to Question 42

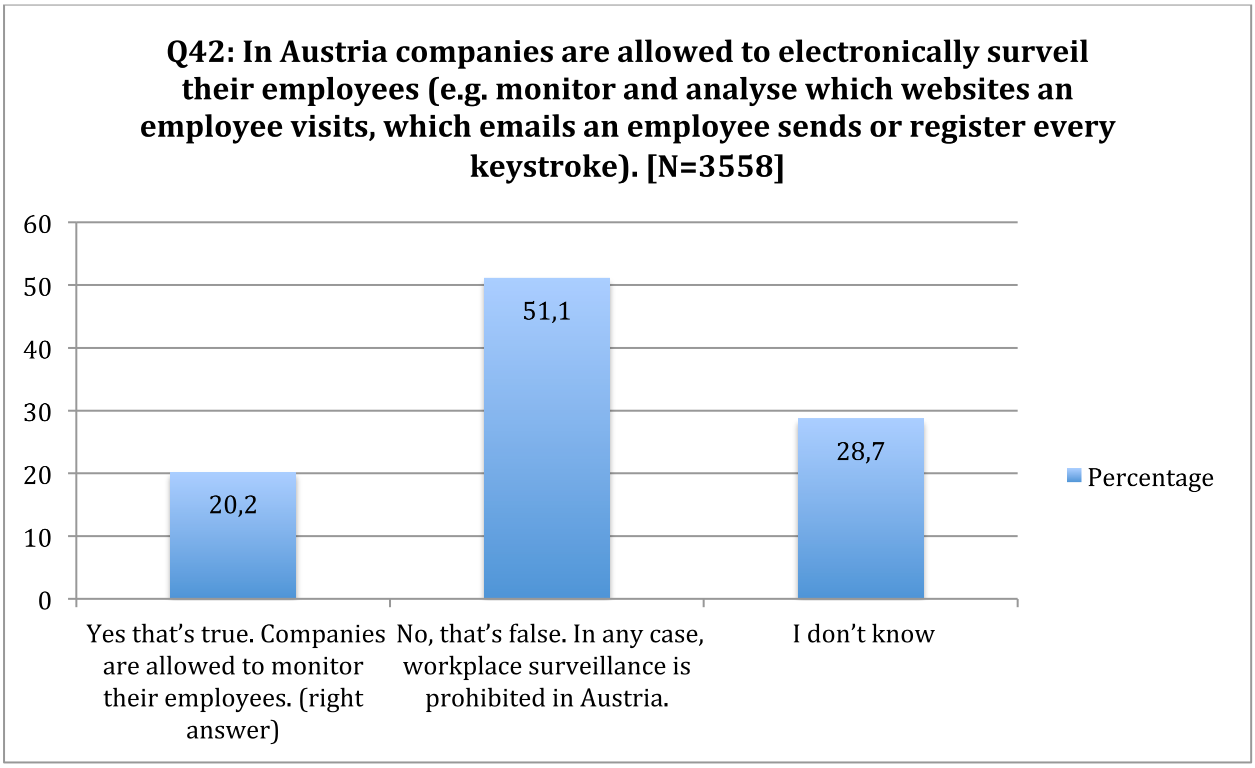


Figure 38: Results to Question 42

4.2.1 Surveillance Knowledge Index

In order to measure surveillance knowledge, we have created a "surveillance knowledge index", which is calculated based on the amount of correct answers to respective questions. For each right answer, we assigned 10 points; for each wrong answer, we assigned 1 point; for “I don’t know” no points were assigned. Thereby, in contrast to existing studies, not only a total score on the surveillance knowledge scale could be obtained, but we could also take into account the ratio between right and wrong answers (and “I don’t know”) as well as easily identify and differentiate between those who scored specifically high on correct or incorrect answers.

For example:

Person A’s score: 40

- 4 correct answers
- 0 incorrect answer
- 4 I don’t know

Person B’s score: 35

- 3 correct answers
- 5 incorrect answers
- 0 I don’t know

Though the overall score does not differ much, there are clear differences in surveillance knowledge between person A and B. Therefore we are able to e.g. identify those, who are characterized by a specifically high score in “false knowledge” and can check for correlation with their field of study, age, social class etc.

	0	10	20	30	40	50	60	70	80
0	0	10	20	30	40	50	60	70	80
1	1	11	21	31	41	51	61	71	
2	2	12	22	32	42	52	62		
3	3	13	23	33	43	53			
4	4	14	24	34	44				
5	5	15	25	35					
6	6	16	26						
7	7	17							
8	8								

High surveillance knowledge (60, 70, 80, 61, 71)

Rather high surveillance knowledge (40, 50, 41, 51, 52, 62, 53)
Rather low surveillance knowledge (20, 30, 21, 31, 32, 42, 33, 43, 44)
Low surveillance knowledge (0, 10, 11, 12, 22, 13, 23, 24, 34, 35)
Wrongful surveillance knowledge (1, 2, 3, 4, 14, 5, 15, 25, 6, 16, 26, 7, 17, 8)

Table 37: Surveillance Knowledge Index Coding Scheme

The following tables summarize the results for the Surveillance Knowledge Index. They show that 75.6% of the respondents have rather low or even less surveillance knowledge. The mode is 32 and therefore lies within the index category of "rather low surveillance knowledge". Only 24.3 % of the respondents have rather high or high knowledge about surveillance on Social Networking Sites, as well as surveillance in general.

Surveillance Knowledge Index

N	Valid	3558
	Missing	0
Mode		32,00
Std. Deviation		13,26301
Minimum		,00
Maximum		80,00

Table 38: Surveillance Knowledge Index (Mode, Std.Deviation, Min, Max)

	Frequency	Percentage
Wrongful Surveillance Knowledge	175	4,9
Low Surveillance Knowledge	876	24,6
Rather low Surveillance Knowledge	1636	46,1
Rather high Surveillance Knowledge	764	21,4
High Surveillance Knowledge	107	2,9

Table 39: Surveillance Knowledge Index Results

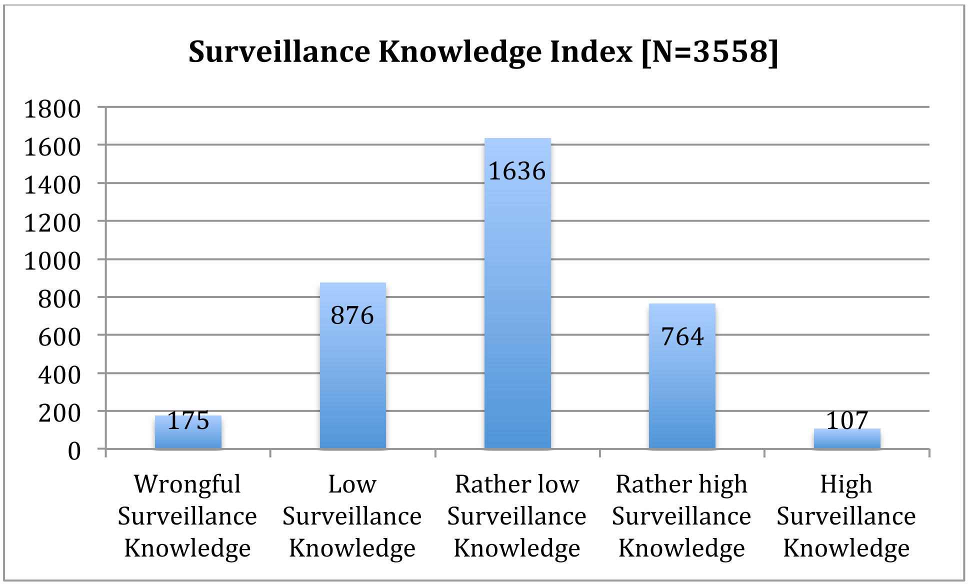


Figure 39: Surveillance Knowledge Index Distribution

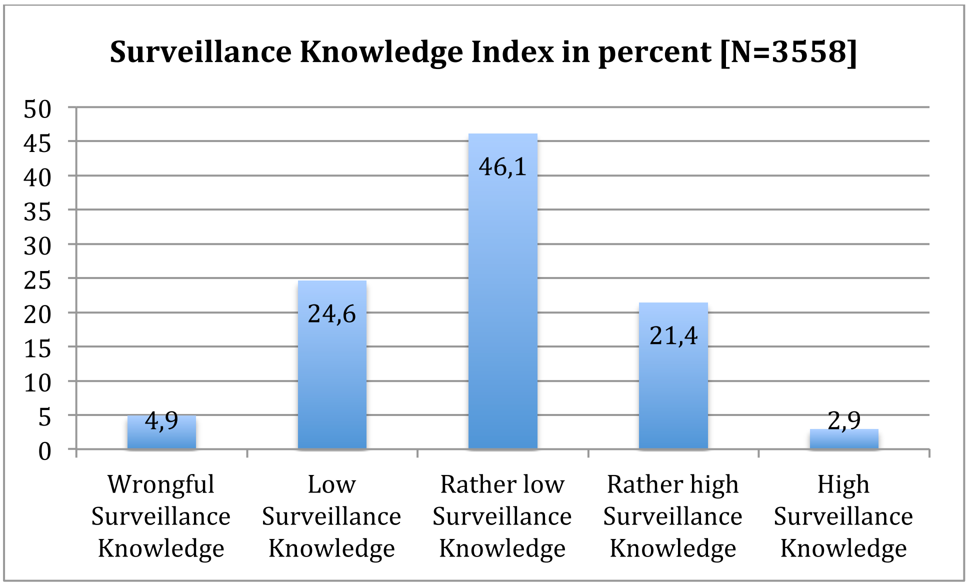


Figure 40: Surveillance Knowledge Index Distribution in percent

The following table shows in detail the results for the Index. It displays how many respondents reached each single score. The values 6, 7, and 8 are not listed, since none of the respondents scored them.

Surveillance Knowledge Index

		Frequency	Percent	Cumulative Percent
Valid	,00	23	,6	,6
	1,00	2	,1	,7

	2,00	8	,2	,9
	3,00	5	,1	1,1
	4,00	7	,2	1,3
	5,00	2	,1	1,3
	10,00	36	1,0	2,3
	11,00	28	,8	3,1
	12,00	38	1,1	4,2
	13,00	42	1,2	5,4
	14,00	35	1,0	6,4
	15,00	31	,9	7,2
	16,00	10	,3	7,5
	17,00	5	,1	7,6
	20,00	60	1,7	9,3
	21,00	96	2,7	12,0
	22,00	139	3,9	15,9
	23,00	160	4,5	20,4
	24,00	120	3,4	23,8
	25,00	51	1,4	25,2
	26,00	19	,5	25,8
	30,00	66	1,9	27,6
	31,00	144	4,0	31,7
	32,00	276	7,8	39,4
	33,00	271	7,6	47,0
	34,00	196	5,5	52,6
	35,00	94	2,6	55,2
	40,00	55	1,5	56,7
	41,00	139	3,9	60,7
	42,00	258	7,3	67,9
	43,00	271	7,6	75,5
	44,00	194	5,5	81,0
	50,00	27	,8	81,7
	51,00	83	2,3	84,1
	52,00	177	5,0	89,0
	53,00	186	5,2	94,3
	60,00	16	,4	94,7
	61,00	57	1,6	96,3
	62,00	97	2,7	99,0
	70,00	4	,1	99,2

	71,00	26	,7	99,9
	80,00	4	,1	100,0
	Total	3558	100,0	

Table 40: Surveillance Knowledge Index Results for Each Score

4.2.2 Correlations

In order to check for any statistically significant associations between the surveillance knowledge index and gender, we calculated the contingency coefficient (C = 0,167). This table shows that male respondents scored higher on the Surveillance Knowledge Index, meaning they had better Surveillance Knowledge.

Gender * Surveillance Knowledge Index Crosstabulation

		Surveillance Knowledge Index					Total
		High	Rather high	Rather low	Low	Wrongful	
Gender:	female	1,9% (44)	17,5% (398)	47,5% (1078)	27,3% (619)	5,8% (131)	100% (2270)
	male	4,9% (63)	28,4% (366)	43,3% (558)	20,0% (257)	3,4% (44)	100% (1288)
Total		3% (107)	21,5% (764)	46,0% (1636)	24,6% (876)	4,9% (175)	100% (3558)

Table 41: Crosstabulation Surveillance Knowledge Index with Gender;
in orange: values above average, in blue: values below average

Correlating the Surveillance Knowledge Index with age, we received a correlation coefficient of -.039. With 1.00 assigned as the perfect positive correlation and -1.00 as the prefect negative correlation, this value represents no (or a very weak) relationship. When the -0.039 is squared to provide the r-squared value, the number calculated is 0.001521, which suggests that age have a very weak influence on the surveillance knowledge index of 0.15%.

Surveillance Knowledge Index * Age Correlations

		Age
Age	Correlation Coefficient (Spearman's Rho)	1
	Sig. (2-tailed)	
	N	3558

Surveillance Knowledge Index	Correlation Coefficient (Spearman's Rho)	-,050*
	Sig. (2-tailed)	,019
	N	3558

*. Correlation is significant at the 0.05 level (2-tailed).

Table 42: Correlation Surveillance Knowledge Index with Age

There was also no correlation observable between the surveillance knowledge index and the level of study (i.e. if someone is doing his/her bachelor, master or phd studies) and only a very weak correlation between the surveillance knowledge index and the monthly income of a participant (see tables 17 and 18). Spearman's rho shows a correlation coefficient of only 0.002 for the level of study, and of 0.068 for the income.

Surveillance Knowledge Index * Level of Study Correlations

		Surveillance Knowledge Index
Surveillance Knowledge Index	Correlation Coefficient	1,000
	Sig. (2-tailed)	.
	N	3558
Level of Study	Correlation Coefficient	,002
	Sig. (2-tailed)	,888
	N	3558

Table 43: Correlation Surveillance Knowledge Index with Level of Study

Surveillance Knowledge Index * Average Monthly Income Correlations

		Surveillance Knowledge Index
Surveillance Knowledge Index	Correlation Coefficient	1,000
	Sig. (2-tailed)	.
	N	3558
Average Monthly Income	Correlation Coefficient	-,068**
	Sig. (2-tailed)	,000
	N	3553

**. Correlation is significant at the 0.01 level (2-tailed).

Table 44: Correlation Surveillance Knowledge Index with Average Monthly Income

The correlation coefficient for a correlation of the surveillance knowledge index with the variables "parental educational level" and "parental occupational status" also showed very weak to no association between these variables (see tables 19 and 20).

Surveillance Knowledge Index * Parental Educational Level Correlations

		Surveillance Knowledge Index
Father's Educational Level	Correlation Coefficient	-,002
	Sig. (2-tailed)	,893
	N	3558
Mother's Educational Level	Correlation Coefficient	,006
	Sig. (2-tailed)	,725
	N	3558

Table 45: Correlation Surveillance Knowledge Index with Parental Educational Level

Surveillance Knowledge Index * Parental Occupational Status Correlations

		Surveillance Knowledge Index
Father's Occupational Status	Correlation Coefficient	-,025
	Sig. (2-tailed)	,132
	N	3558
Mother's Occupational	Correlation Coefficient	-,013
	Sig. (2-tailed)	,439

Status	N	3558

Table 46: Correlation Surveillance Knowledge Index with Parental Occupational Status

Hypothesis 8: More knowledge about surveillance is significantly positively correlated to more careful information behaviour on SNS (intensity of reading the terms of use, degree of deactivation of advertising options, degree of activation of privacy mechanisms).

Correlation analysis shows that there is a significantly negative correlation between the Surveillance Knowledge Index and the Carefulness Index. Since a high score on the Carefulness Index indicates a more careful behavior, and a low score on the Surveillance Knowledge Index stands for higher knowledge, this means that hypothesis 8 has been validated.

Careful Information Behaviour * Surveillance Knowledge Correlations

		Surveillance Knowledge Index	Carefulness Index
Surveillance Knowledge Index	Correlation Coefficient	1	-,085**
	Sig. (2-tailed)		,000
	N	3558	3558
Carefulness Index	Correlation Coefficient	-,085**	1
	Sig. (2-tailed)	,000	
	N	3558	3558

**. Correlation is significant at the 0.01 level (2-tailed).

Table 47: Correlation Surveillance Knowledge with Careful Information Behaviour

Hypothesis 9: A more critical attitude towards surveillance is significantly positively correlated to more careful information behaviour on SNS (intensity of reading the terms of use, degree of deactivation of advertising options, degree of activation of privacy mechanisms).

In order to assess this hypothesis it is necessary to clarify what "critical attitude towards surveillance" means and how it can be operationalized:

4.3 Variable #3: Critical Attitude towards Surveillance

As already mentioned above (see hypothesis #8) we are especially interested in users' critical attitudes towards surveillance by economic actors, but will also evaluate attitudes towards surveillance in general. We will test in how far students consider surveillance as an actual problem or if they do not think of it as a problem at all.

In the pilot study conducted among students at Salzburg University, Fuchs (2009, 61) found that gender, type and extension of higher education, class and usage frequency of social networking sites are factors that influence the degree of critical attitude towards surveillance.

Users of social networking sites are concerned about "disclosure of personal information, damaged reputation due to rumours and gossip, unwanted contact and harassment or stalking, surveillance-like structures due to backtracking functions, use of personal data by third-parties, and hacking and identity theft" (Debatin et al. 2009, 84) Existing studies also show that students are explicitly critical towards surveillance conducted by their current or potentials employers, whom they do not want to see personal information posted on Facebook (Christofides, Muise, and Desmarais 2009, 341; Peluchette and Karl 2008). Dommeyer and Gross (2003) conducted a study in order to examine consumer's awareness and use of strategies that may protect consumers' privacy from marketing practices. Among others they tested the hypothesis that "there will be a negative association between a person's desire to receive solicitation from direct marketers (…) and usage of privacy protection strategies" (Dommeyer and Gross 2003, 40). The results largely supported this hypothesis, suggesting that consumers who are most critical against direct marketing solicitations will be most motivated to adopt privacy protection strategies.

Therefore we hypothesize that users who show a more critical attitude towards surveillance by economic actors, but also surveillance in general, are more likely to show careful information behaviour on social networking sites.

Though we were especially interested in users' critical attitudes towards surveillance by economic actors, we have also evaluated attitudes towards surveillance in general. We tested in how far students consider surveillance as an actual problem or if they do not think of it as a problem at all.

We operationalized the variable "Critical Attitude towards Surveillance" by measuring the degree of agreement (using a likert-scale) with five different statements:

- "If you have nothing illegal to hide, then you need not be afraid of surveillance"
- "We need more surveillance in order to protect ourselves from increasing crime, sex predators, and terrorists so as to be able to live in safety."
- "It won't hurt me if companies know personal information about me."
- "It is OK, that companies screen job applicants on the Internet (e.g. on social networking sites) and search for personal information in order to reach a decision."
- "Imagine that in the course of a routine test a hospital determines that you are overweight. You think it is OK that your data is passed on to health companies, which send you offers for nutrition seminars and fitness trainings."

Participants were asked to indicate their agreement/disagreement with the presented statements on a scale from 1 to 5, with 5 being the most surveillance-critical answer, and 1 being the least surveillance-critical answer.

By use of the Likert Method of Summated Ratings the collected data is analysed. All the answers put together, the highest possible value is 25, the lowest possible result is 5. Based on the results we constructed a surveillance critique index, which allows us to correlate it with other variables, such as sociodemographic data or information behaviour.

25 – 21	Very Critical (towards surveillance)
20 – 16	Critical (towards surveillance)
15 – 11	Slightly Critical (towards surveillance)
10 - 5	Not Critical (towards surveillance)

Table 48: Surveillance Critique Index Categories

Findings from our study show that students tend to have quite a critical attitude towards surveillance. When presented the five statements, in most cases respondents answered with disagreement or even total disagreement on the 5 point Likert-Scale, which meant a more critical standpoint towards surveillance. Especially for Q47, more than 50% of the respondents clearly stated their total disagreement with the presented statement about highly targeted advertising by use of sensitive personal data ("Imagine that in the course of a routine test a hospital determines that you are overweight. You think it is OK that your data is passed on to health companies, which send you offers for nutrition seminars and fitness trainings."). Another 27.9% disagreed with the statement, which means that a total of more than 80% were highly critical towards such an approach. Only 7.3% of the respondents thought it was OK for health companies to target their customers this way. Accordingly, for all other statements more than a majority checked that they “don’t agree” or “don’t agree at all”. The statement, which triggered the most neutral responses (32%), was Q44 “We need more surveillance in order to protect ourselves from increasing crime, sex predators, and terrorists so as to be able to live in safety.“ Interestingly, respondents’ answers were the least critical in Q46 “It is OK, that companies screen job applicants on the Internet (e.g. on social networking sites) and search for personal information in order to reach a decision.” Over 23% of the respondents agreed or totally agreed with this statement, which was the highest amount for all statements. However, even here a total of about 53% was critical about such practices and disagreed or disagreed at all with the statement.

Statistics

		Q43	Q44	Q45	Q46	Q47
N	Valid	3558	3558	3558	3558	3558
	Missing	0	0	0	0	0
Mean		2,1998	2,4862	2,0790	2,4531	1,7496
Mode		2,00	3,00	2,00	1,00	1,00
Std. Deviation		1,11333	1,07712	,93096	1,22039	,96376
Variance		1,240	1,160	,867	1,489	,929
Minimum		1,00	1,00	1,00	1,00	1,00
Maximum		5,00	5,00	5,00	5,00	5,00

Table 49: Results to Questions 43-47

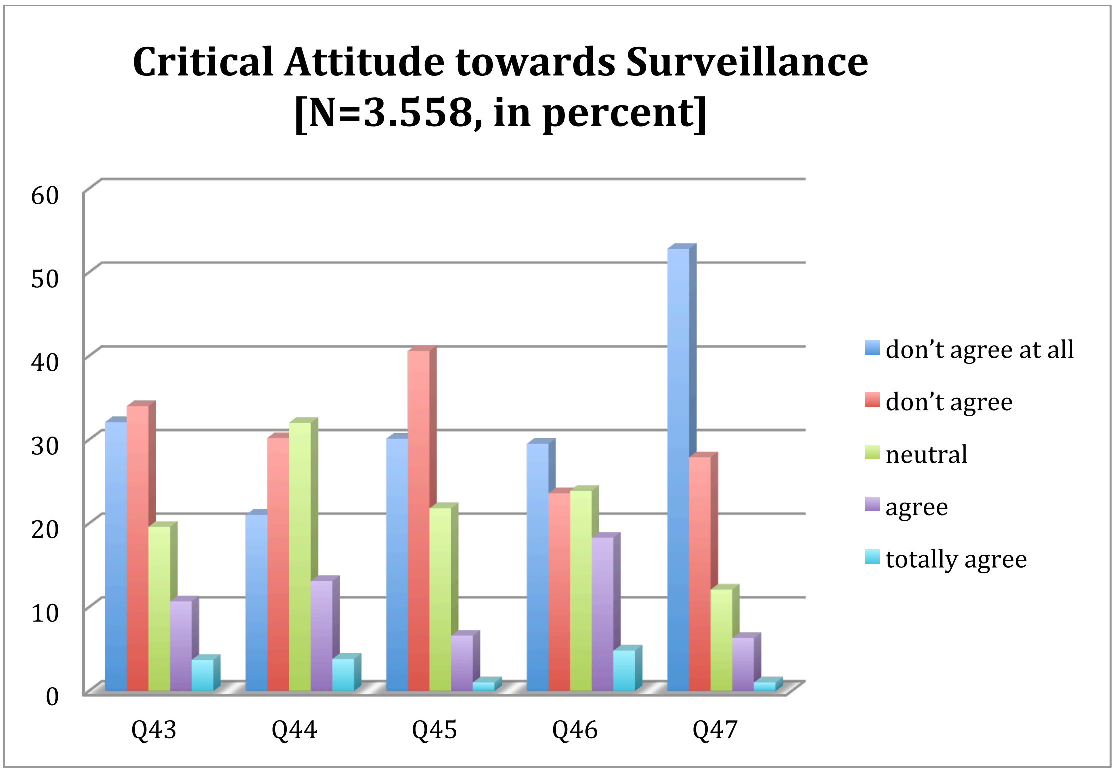
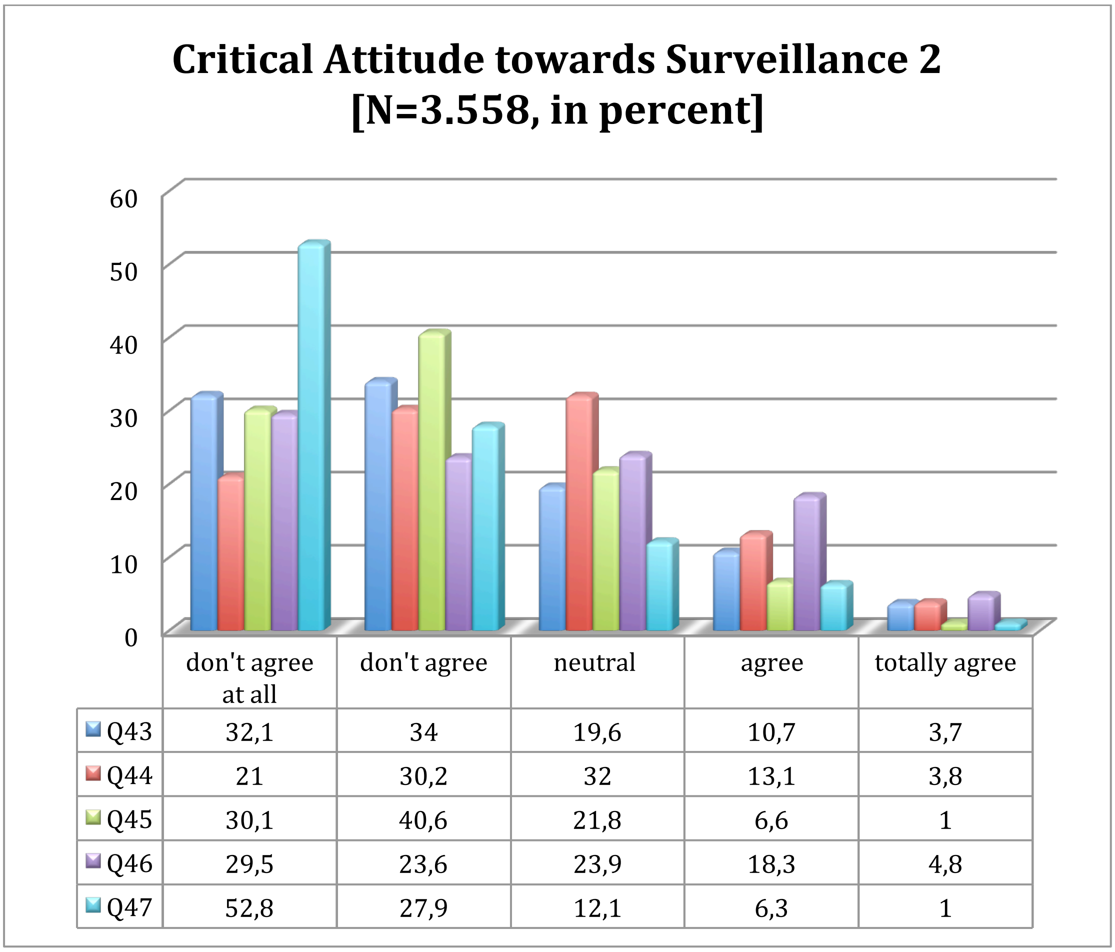


Figure 41: Results to Questions 43-47

(Q43: If you have nothing illegal to hide, then you need not be afraid of surveillance
Q44: We need more surveillance in order to protect ourselves from increasing crime, sex predators, and terrorists so as to be able to live in safety.
Q45: It won't hurt me if companies know personal information about me.
Q46: It is OK, that companies screen job applicants on the Internet (e.g. on social networking sites) and search for personal information in order to reach a decision.
Q47: Imagine that in the course of a routine test a hospital determines that you are overweight. You think it is OK that your data is passed on to health companies, which send you offers for nutrition seminars and fitness trainings.)

The following chart compares the single answer categories (don't agree at all – total agree) for all statements:



	don't agree at all	don't agree	neutral	agree	totally agree
Q43	32,1	34	19,6	10,7	3,7
Q44	21	30,2	32	13,1	3,8
Q45	30,1	40,6	21,8	6,6	1
Q46	29,5	23,6	23,9	18,3	4,8
Q47	52,8	27,9	12,1	6,3	1

Figure 42: Comparison of results to Questions 43-47
(Q43: If you have nothing illegal to hide, then you need not be afraid of surveillance
Q44: We need more surveillance in order to protect ourselves from increasing crime, sex predators, and terrorists so as to be able to live in safety.
Q45: It won't hurt me if companies know personal information about me.
Q46: It is OK, that companies screen job applicants on the Internet (e.g. on social networking sites) and search for personal information in order to reach a decision.
Q47: Imagine that in the course of a routine test a hospital determines that you are overweight. You think it is OK that your data is passed on to health companies, which send you offers for nutrition seminars and fitness trainings.)

4.3.1 Surveillance Critique Index

In the next step we calculated the Surveillance Critique Index as described above. The results were consistent with the impression we got from analysing the single statements. Respondents in our study seem to be quite critical in their attitude towards surveillance. The Mean of the Index is 19, which means that the average student in our survey is critical towards surveillance. The Mean is even close to the next and highest category in our Index (21-25 very critical towards surveillance). Though, among the results also the highest and lowest possible values are represented, the standard deviation only accounts for 3.49 and supports the finding that respondents are rather critical.

Statistics

N	Valid	3558
	Missing	0
Mean		19,0323
Std. Deviation		3,48801
Variance		12,166
Minimum		5,00
Maximum		25,00

Table 50: Surveillance Critique Index (Mean, Std. Deviation, Variance, Min,.,Max.)

In the following table all the results and their distribution are illustrated in detail. The different Index levels are marked with colour.

Surveillance Critique Index

		Frequency	Percent	Cumulative Percent
Valid	5,00	1	,0	,0
	7,00	3	,1	,1
	8,00	6	,2	,3
	9,00	19	,5	,8
	10,00	22	,6	1,4
	11,00	37	1,0	2,5
	12,00	54	1,5	4,0
	13,00	102	2,9	6,9
	14,00	120	3,4	10,2
	15,00	212	6,0	16,2
	16,00	245	6,9	23,1
	17,00	258	7,3	30,3

18,00	368	10,3	40,7
19,00	426	12,0	52,6
20,00	448	12,6	65,2
21,00	360	10,1	75,4
22,00	268	7,5	82,9
23,00	265	7,4	90,3
24,00	124	3,5	93,8
25,00	220	6,2	100,0
Total	3558	100,0	

Table 51: Surveillance Critique Index - results for each score

Summarized with the four categories of the Surveillance Critique Index we obtained the following results:

Surveillance Critique Index

	Frequency	Percent	Cumulative Percent
not critical	51	1,4	1,4
slightly critical	525	14,8	16,2
critical	1745	49,0	65,2
very critical	1237	34,8	100,0
Total	3558	100,0	

Table 52: Surveillance Critique Index

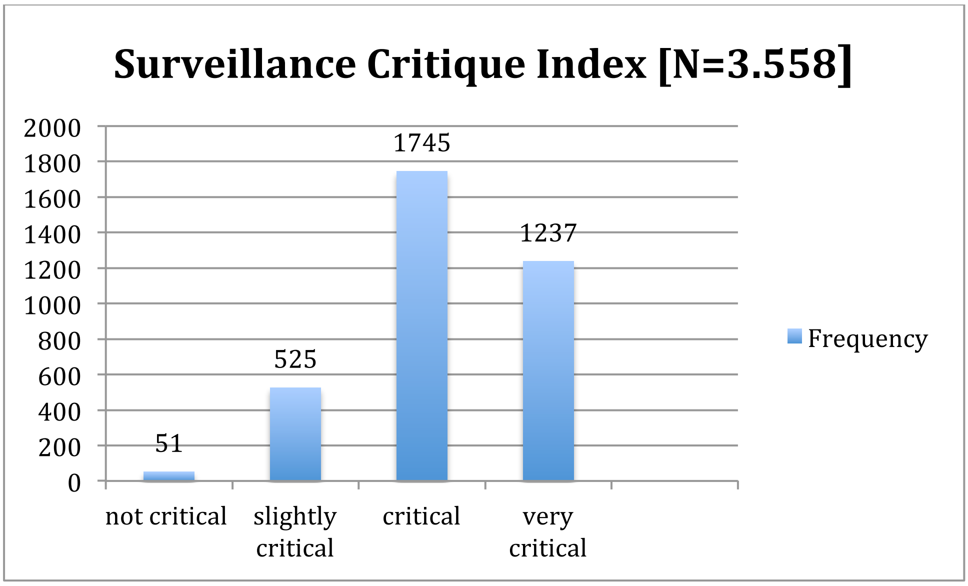


Figure 43: Surveillance Critique Index Distribution

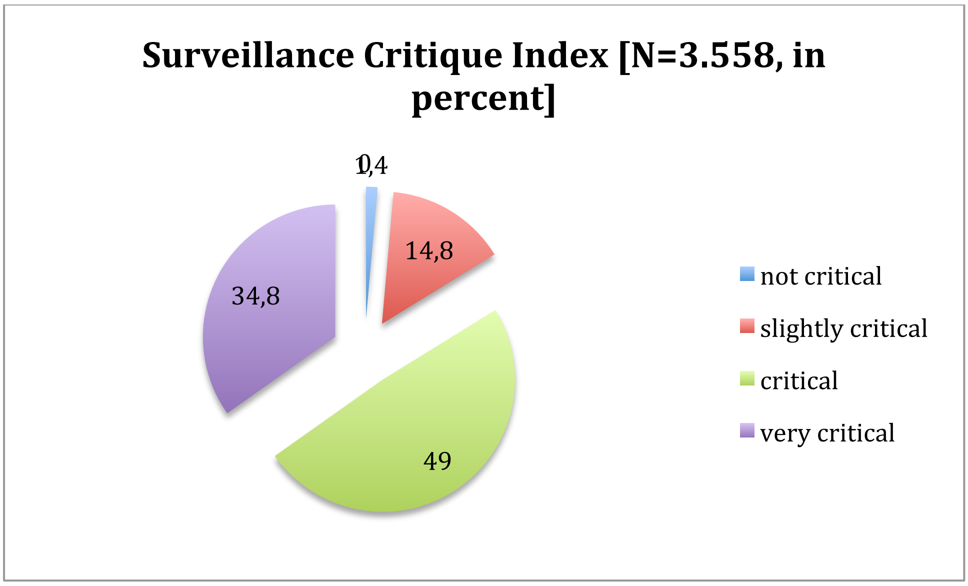


Figure 44: Surveillance Critique Index Distribution in percent

In the following, the results (percentage and frequency) for each of the five statements are shown in detail. Results are rounded up to one decimal point.

Q43: If you have nothing illegal to hide, then you need not be afraid of surveillance.

		Frequency	Percent	Cumulative Percent
Valid	don't agree at all	1142	32,1	32,1
	don't agree	1208	34,0	66,0
	neutral	696	19,6	85,6
	agree	379	10,7	96,3
	totally agree	133	3,7	100,0
	Total	3558	100,0	

Table 53: Results to Question 43

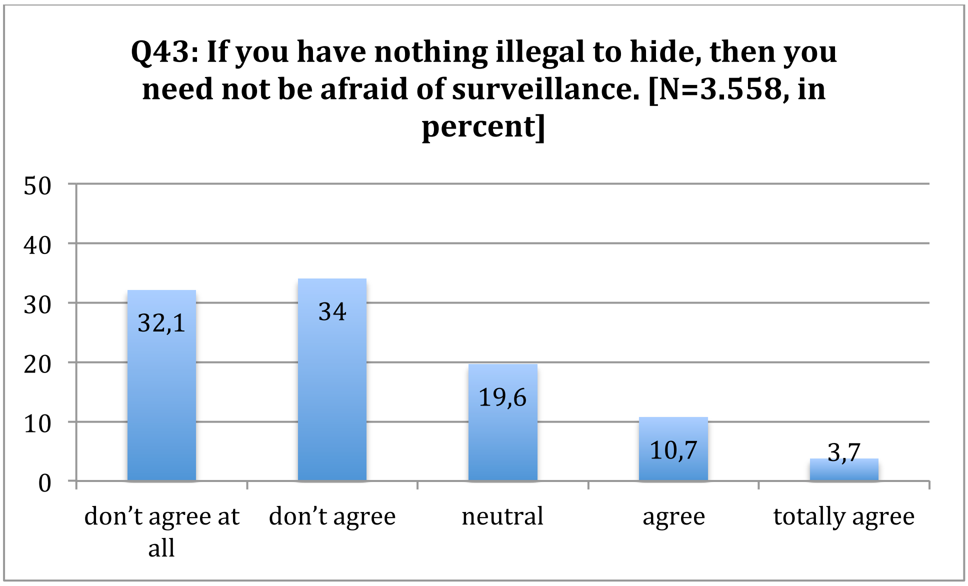


Figure 45: Results to Question 43

Q44: We need more surveillance in order to protect ourselves from increasing crime, sex predators, and terrorists so as to be able to live in safety.

		Frequency	Percent	Cumulative Percent
Valid	don't agree at all	746	21,0	21,0
	don't agree	1073	30,2	51,1
	neutral	1138	32,0	83,1
	agree	465	13,1	96,2
	totally agree	136	3,8	100,0
	Total	3558	100,0	

Table 54: Results to Question 44

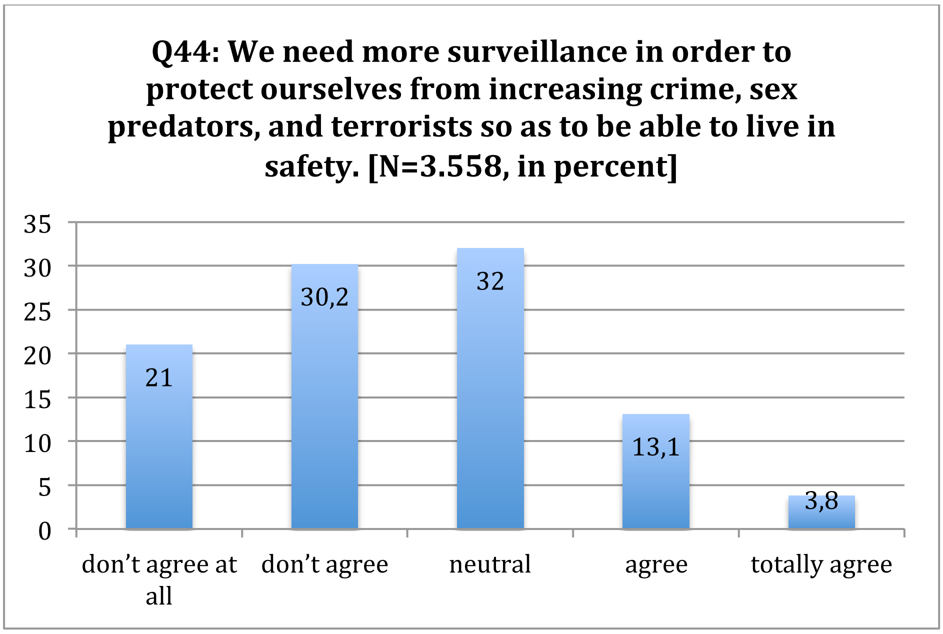


Figure 46: Results to Question 44

Q45: It won't hurt me if companies know personal information about me.

		Frequency	Percent	Cumulative Percent
Valid	don't agree at all	1070	30,1	30,1
	don't agree	1443	40,6	70,6
	neutral	775	21,8	92,4
	agree	234	6,6	99,0
	totally agree	36	1,0	100,0
	Total	3558	100,0	

Table 55: Results to Question 45

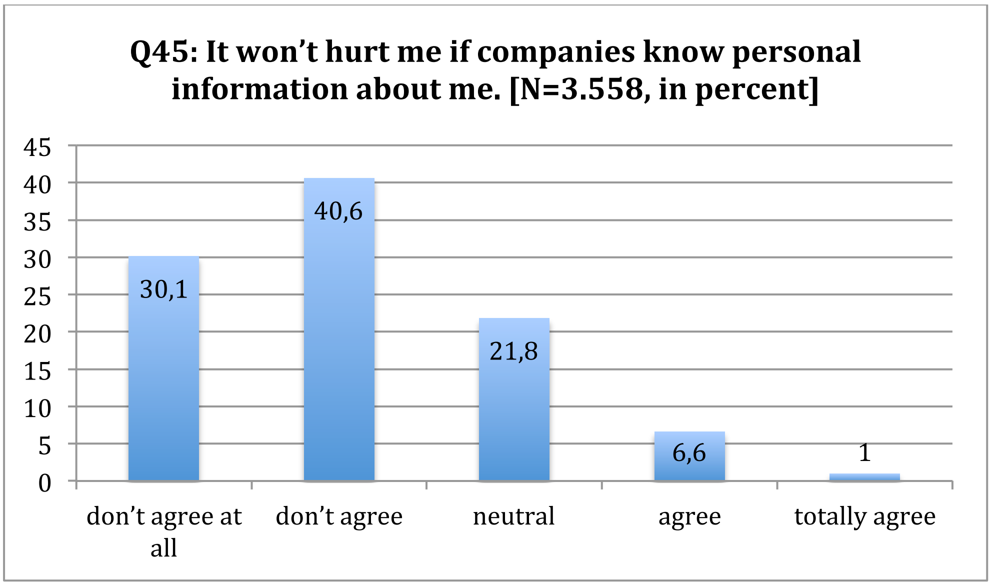


Figure 47: Results to Question 45

Q46: It is OK, that companies screen job applicants on the Internet (e.g. on social networking sites) and search for personal information in order to reach a decision.

		Frequency	Percent	Cumulative Percent
Valid	don't agree at all	1048	29,5	29,5
	don't agree	840	23,6	53,1
	neutral	850	23,9	77,0
	agree	650	18,3	95,2
	totally agree	170	4,8	100,0
	Total	3558	100,0	

Table 56: Results to Question 46

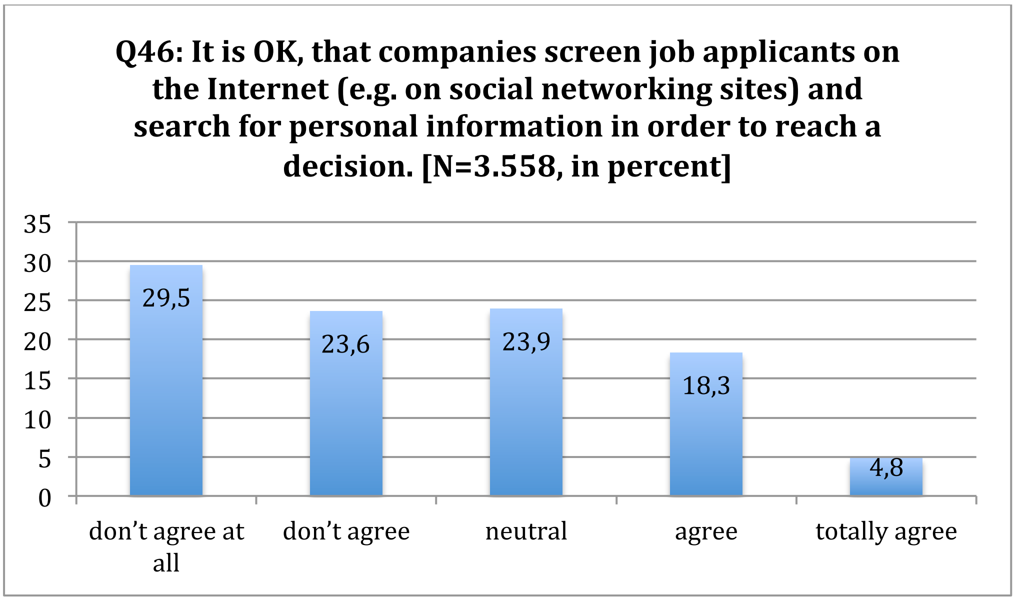


Figure 48: Results to Question 46

Q47: Imagine that in the course of a routine test a hospital determines that you are overweight. You think it is OK that your data is passed on to health companies, which send you offers for nutrition seminars and fitness trainings.

		Frequency	Percent	Cumulative Percent
Valid	don't agree at all	1877	52,8	52,8
	don't agree	991	27,9	80,6
	neutral	430	12,1	92,7
	agree	224	6,3	99,0
	totally agree	36	1,0	100,0
	Total	3558	100,0	

Table 57: Results to Question 47

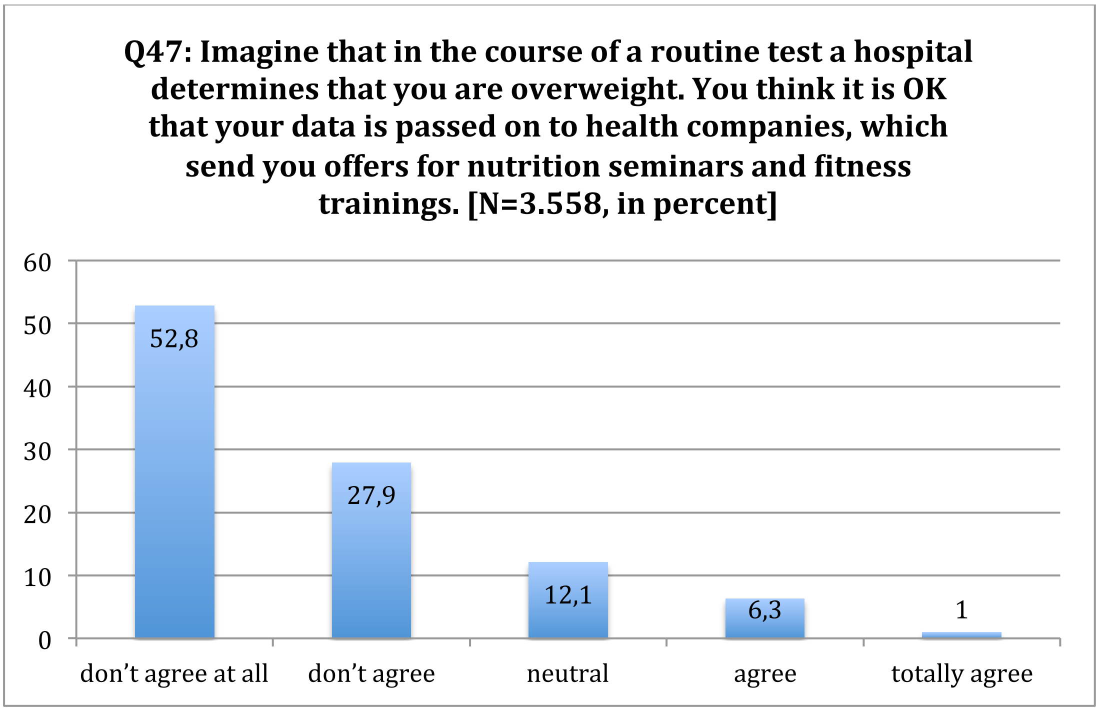


Figure 49: Results to Question 47

4.3.2 Correlations

A correlation analysis (point biserial for gender, Pearson's correlation for age and Spearman rank order for ordinal variables) was run to determine the relationship between the Surveillance Critique Index and some demographic variables.

We found weak positive correlations between this index and gender (male respondents show a more critical attitude towards surveillance than female participants), as well as age and the educational level of the respondents' mothers, which were statistically significant. There was no statistically significant association between the surveillance critique index and the level of study, the average monthly income, as well as the parental occupational status and the paternal level of education (see tables 31 and 32).

Correlations

		Surveillance Critique Index
Gender	Correlation Coefficient (r_{pb})	,066**
	Sig. (2-tailed)	,000
	N	3558

Age	Correlation Coefficient (Pearson)	,038**
	Sig. (2-tailed)	,000
	N	3558
Level of Study	Correlation Coefficient (Spearman's Rho)	,008
	Sig. (2-tailed)	,634
	N	3558
Average Monthly Income	Correlation Coefficient (Spearman's Rho)	,021
	Sig. (2-tailed)	,220
	N	3553

**. Correlation is significant at the 0.01 level (2-tailed).

Table 58: Correlation Surveillance Critique Index with demographic variables

Correlations

		Surveillance Critique Index
Father's Educational Level	Correlation Coefficient (Spearman's Rho)	,027
	Sig. (2-tailed)	,106
	N	3558
Mother's Educational Level	Correlation Coefficient (Spearman's Rho)	,045**
	Sig. (2-tailed)	,008
	N	3558
Father's Occupational Status	Correlation Coefficient (Spearman's Rho)	,008
	Sig. (2-tailed)	,617
	N	3558
Mother's Occupational Status	Correlation Coefficient (Spearman's Rho)	,012
	Sig. (2-tailed)	,460
	N	3558

**. Correlation is significant at the 0.01 level (2-tailed).

Table 59: Correlation Surveillance Critique Index with parental educational and occupational status

Correlation analysis shows that there is some significant relation between the critical attitude towards surveillance of our respondents and the intensity of their usage behavior. With a negative spearman's rho of -0.99, respondents that are classified as heavy users of Facebook are significantly positively correlated to a less critical attitude towards surveillance. Participants that show a less intense usage behavior are associated with a more critical attitude towards surveillance.

Intensity of Usage* Surveillance Critique Index Correlations

		Intensity Index	Surveillance Critique Index
Intensity Index	Correlation Coefficient (Spearman's Rho)	1,000	-,099**
	Sig. (2-tailed)	.	,000
	N	3558	3558
Surveillance Critique Index	Correlation Coefficient (Spearman's Rho)	-,099**	1,000
	Sig. (2-tailed)	,000	.
	N	3558	3558

**. Correlation is significant at the 0.01 level (2-tailed).

Table 60: Correlation Surveillance Critique Index with Intensity of Usage

Hypothesis 9: A more critical attitude towards surveillance is significantly positively correlated to more careful information behaviour on SNS (intensity of reading the terms of use, degree of deactivation of advertising options, degree of activation of privacy mechanisms).

A Spearman's Rank Order correlation was run to determine the relationship between the respondents' critical attitude towards surveillance and their information behaviour. With a correlation coefficient of 0.124 a significantly positive correlation can be observed between a more critical attitude towards surveillance and more critical information behaviour on social networking sites. This means that hypothesis 9 has been validated.

Careful Information Behaviour * Surveillance Critique Index Correlations

		Surveillance Critique Index	Carefulness Index
Surveillance Critique Index	Correlation Coefficient (Spearman's Rho)	1,000	,124**
	Sig. (2-tailed)	.	,000
	N	3558	3558

Carefulness Index	Correlation Coefficient (Spearman's Rho)	,124**	1,000
	Sig. (2-tailed)	,000	.
	N	3558	3558

**. Correlation is significant at the 0.01 level (2-tailed).

Table 61: Correlation Surveillance Critique Index with Careful Information Behaviour

Hypothesis 10: There are significant differences in information behaviour on SNS between students in the hard and the soft sciences.

In order to assess this hypothesis it is necessary to clarify what "hard science vs. soft science" means and how they can be distinguished:

4.4 Variable #4: Field of Study (Hard Science & Soft Science)

The terms "hard science" and "soft science" are often used when distinguishing fields of academic research. "Hard sciences" are considered to be more scientific, mathematically rigorous and concerned with phenomena and "discoveries far removed from routine human experience" (Frost 2009). Hard sciences are characterized as being focused on accuracy, quantifiable data, and objectivity. In contrast soft sciences are concerned with the individual and its relations to society. Soft science is not defined by definite laws, but by different, sometimes opposing views and interpretations of social reality.

There is no definite assignment, but typically fields such as natural sciences or computer sciences are described as "hard sciences", whereas social sciences, such as sociology, communication studies, and political science are referred to as "soft sciences". (Frost 2009)

Hard sciences rely heavily on quantifiable data and positivistic research, whereas soft sciences "also employ more qualitative methods and are more frequently confronted with critical theories and critical research in their studies than natural scientists. Positivism is only interested in how something is, whereas critical thinking is interested in suppressed potentials and in what something could become and how it can be improved. Positivism is instrumental, whereas criticism is noninstrumental" (Fuchs 2009, 64; see also Adorno 1976)

Therefore we assume that students of hard sciences tend to be less critical of social phenomena such as surveillance or threats to privacy. Assuming hypotheses 8 is proven right, (saying that a more critical attitude towards surveillance will be positively correlated with a more careful information behaviour), students of hard sciences will show a less careful information behaviour. On the contrary, studying soft sciences will increase the likelihood of being critical of surveillance, thereby increasing the likelihood of being more careful in providing information on social networking sites.

However we are aware that single study programmes may constitute an exception. For example, we presume that computer sciences may reach higher levels of careful information behaviour. Since surveillance on social networking sites is strongly connected to data collection and electronic data processing, we assume that students of computer sciences are more familiar with both, surveillance technologies and the implementation of privacy protection techniques. If hypothesis no. 7 is proven right, more knowledge increases the likelihood of more careful information behaviour. Hence, students educated in technical aspects of privacy and surveillance will show a more careful information behaviour.

These assumptions are supported by existing findings from a study by Buchanan et al. (2007), who conducted three surveys in order to understand the discourse of Internet users' privacy concerns, and any actions they take to guard against these concerns. In the second survey, the scale validity (developed in survey no.1) was examined by comparing scores from groups considered likely to differ in privacy-protective behaviours. 69 students from the Open University (UK), partly from technology-based studies (38 participants) and partly from social sciences (31 participants), answered a Web-based questionnaire with a refined set of 16 privacy attitude items and 12 privacy behaviour items (Buchanan et al. 2007, 161-162). Overall the technical and non-technical students did not differ significantly in their level of online privacy concern, but did so on the technical protection scale (with the technical students scoring higher), as well as on the general caution scale. Similarly, Milne, Rohm and Bahl (2004) found that though less than a majority of participants of their study use technology for protecting their personal information, the more technically savvy students scored higher at more advanced privacy protection actions such as using anonymizers while browsing or anonymous re-mailers.

Variable #4 was operationalized within the general set of sociodemographic data questions (for the whole set – including question on gender, age, income, duration of study – see Appendix A).

In survey question no. 71 participants were asked to choose from a predefined list, which field of study they pursue. The response options included:

- natural sciences,
- technical sciences and engineering,
- social sciences,
- economics,
- humanities and cultural studies,
- arts,
- theology,
- law,
- medicine,
- agricultural/forest and veterinary sciences,
- sports

Additionally we introduced an open answering category (further/sonstige).

Study fields were categorized as follows:

HARD SCIENCES	SOFT SCIENCES
Natural sciences	Social Sciences

Technical Sciences and Engineering	Economics
Medicine	Humanities and Cultural Studies
Agricultural/Forest and Veterinary Sciences	Arts
Sports	Theology
	Law

Table 62: Field of Study _ Hard vs. Soft Sciences

Based on the results two groups can be identified: respondents that are students of hard sciences and respondents that are students of soft science.

Within these 12 categories we received 4135 answers (multiple answers were possible, since some students have more than one field o f study). From these, 83 respondents checked "other/further". We didn't count these answers, since they referred to very special study fields. Therefore we analysed the remaining 4.052 answers.

The figures below show the distribution of the fields of study in absolute numbers, as well as in percent:

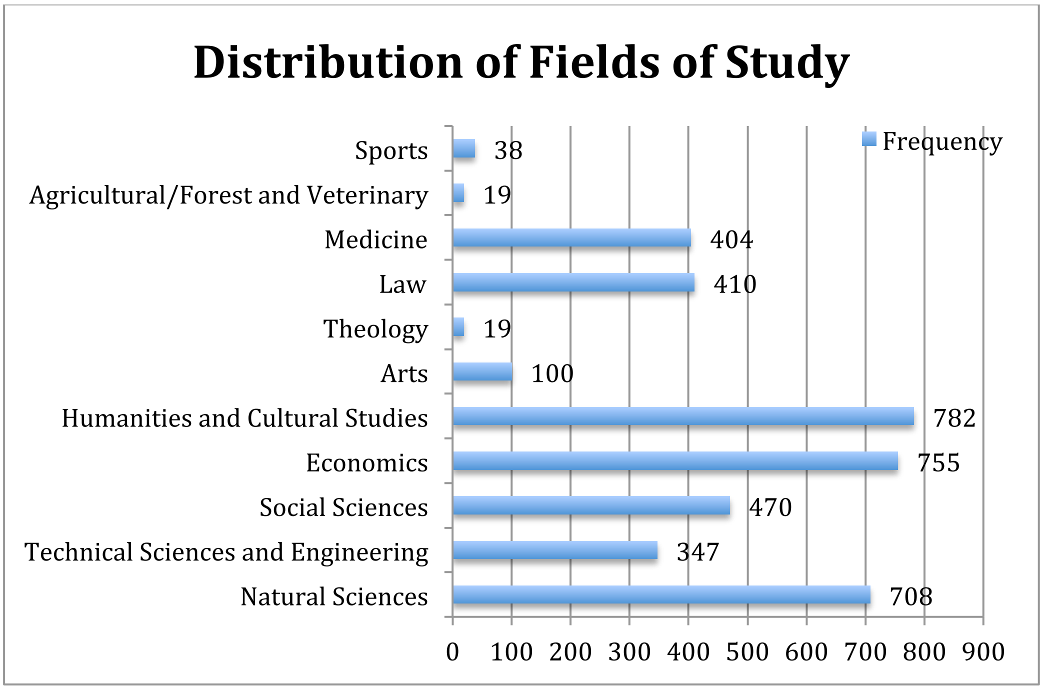


Figure 50: Distribution of Fields of Study (Frequency)

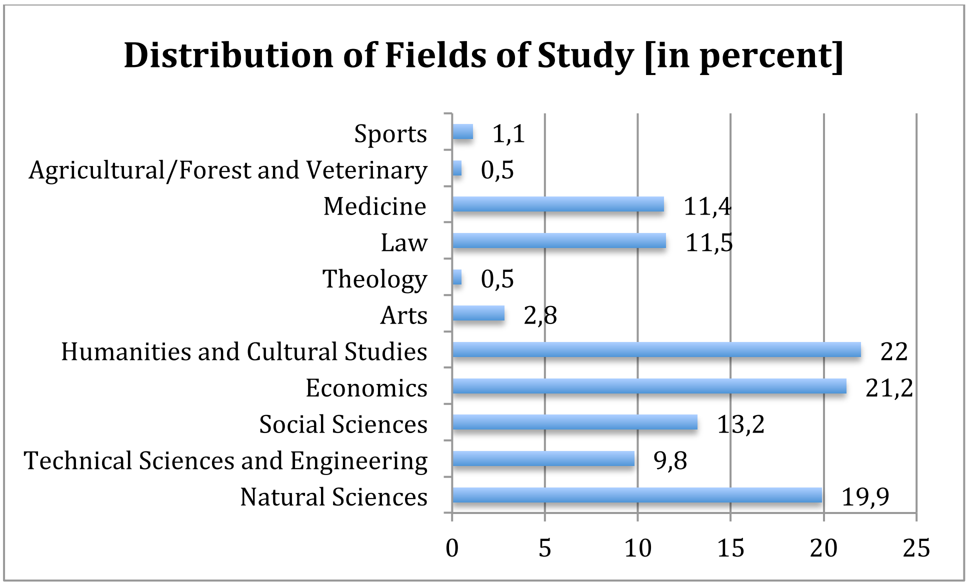


Figure 51: Distribution of Fields of Study (Percentage) 1

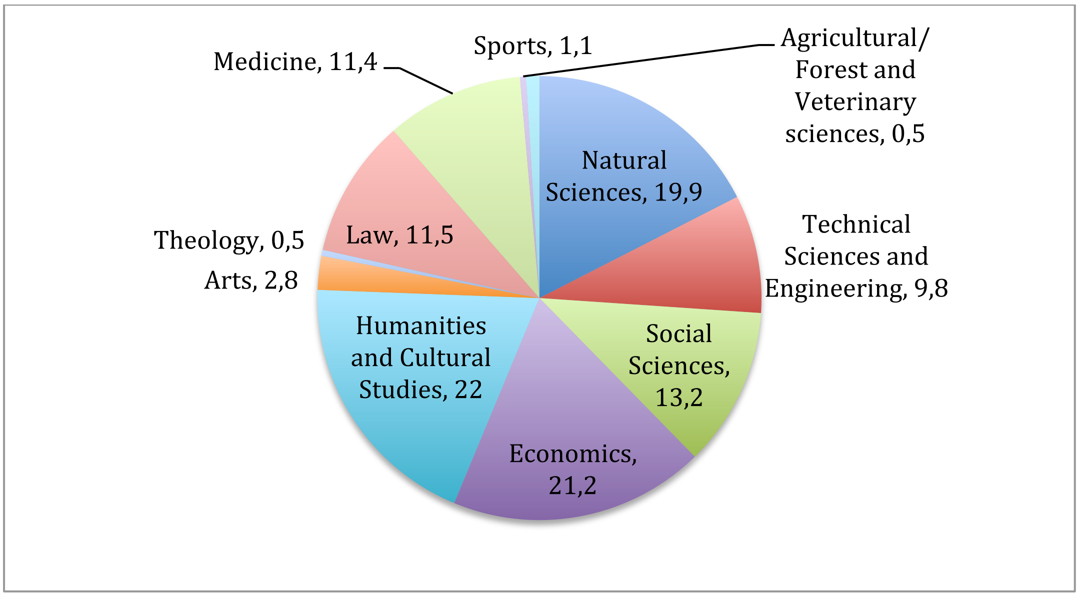


Figure 52: Distribution of Fields of Study (Percentage) 2

In the next step we categorized all answers into the two categories “hard sciences” and “softs sciences” as illustrated above. The table shows that 1.516 of our respondents are students in the field of hard sciences, and 2.536 respondents study within the field of soft sciences.

Hard Sciences		Soft Sciences	
Natural sciences	708	Social Sciences	470
Technical Sciences and Engineering	347	Economics	755
Medicine	404	Humanities and Cultural	782

		Studies	
Agricultural/Forest and Veterinary Sciences	19	Arts	100
Sports	38	Theology	19
		Law	410
Total	1.516		2.536

Table 63: Frequency Distribution for fields of study

Due to the possibility of multiple answers, the distribution is as follows: 2.104 of our respondents study within the field of Soft Sciences, 1.296 of our respondents study within the field of Hard Sciences, and the remaining 158 study in both fields.

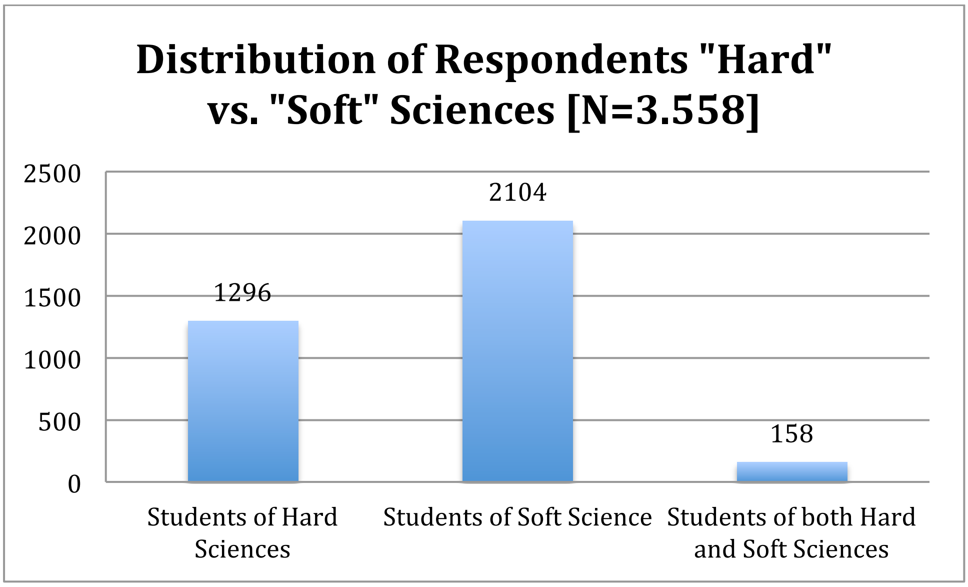


Figure 53: Distribution of Respondents between Hard and Soft Sciences

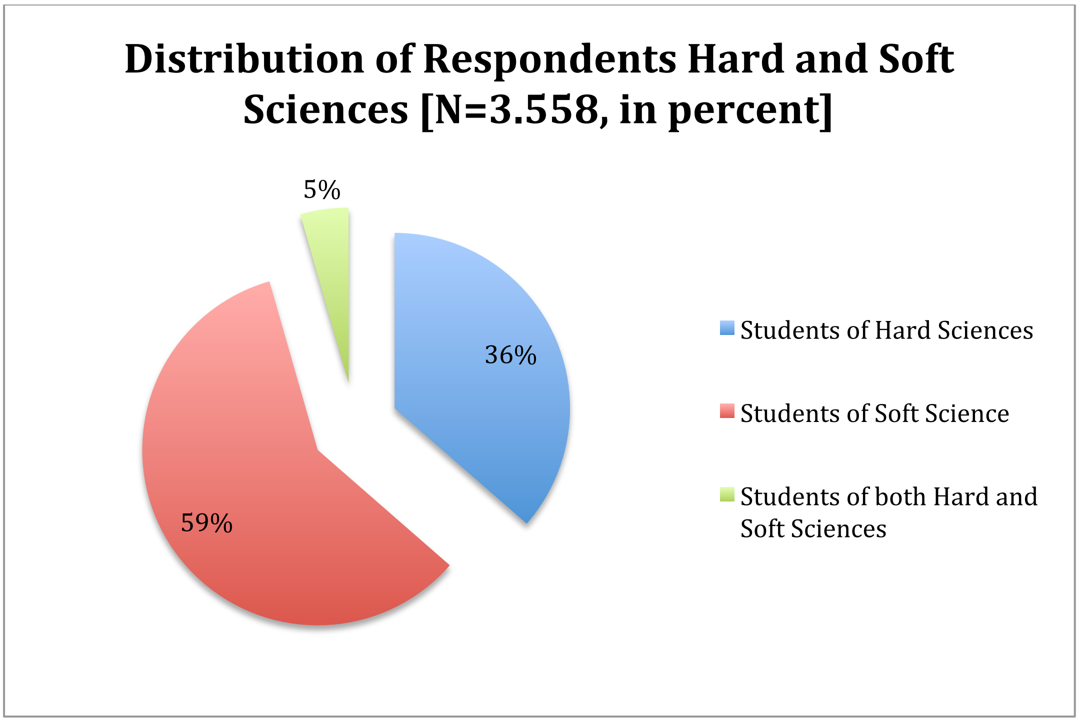


Figure 54: Distribution of Respondents between Hard and Soft Sciences (Percentage)

4.4.1 Correlations

We also checked for any relation between the field of study (hard vs. soft sciences) and the level of surveillance knowledge. Therefore we calculated the results from the surveillance knowledge index against the categorization of the fields of study. Comparing these results with the overall distribution of the respondents among the fields of study, some variations are observable (see table 67), however a Chi Square Test confirmed the null hypothesis (that there is no statistically significant association between the two variables) and Cramer's V value (0,026) was very low accordingly.

		Hard vs. Soft Science		
		Hard Science (1,00)	Soft Science (2,00)	Hard&Soft Science (3,00)
Surveillance Knowledge Index	Very high	39.25 %	55.14 %	5.61 %
	High	38.22 %	57.98 %	3.8 %
	Little	35.82 %	59.54 %	4.65 %
	Poor	36.42 %	58.9 %	4.68 %
	Wrongful	32.57 %	64 %	3.43 %
Total		36.4 %	59.1 %	4.5 %

Table 64: Crosstabulation Surveillance Knowledge Index with Hard/Soft Sciences (Percentage), in orange: values above average; in blue: values beyond average.

Furthermore we analysed if there is any significant relationship between the field of study and other variables. We found a relation between the field of study and gender, implying that more male respondents are studying hard sciences.

Field of Study and Gender

		Value	Approx. Sig.
Nominal by Nominal	Phi	,137	,000
	Cramer's V	,137	,000
N of Valid Cases		3558	

Table 65: Phi and Cramer's V of Field of Study and Gender

Field of Study * Gender: Crosstabulation

		female	male	Total
	Hard Science	55,4% (718)	44,6% (578)	100% (1296)
	Soft Science	69,2% (1456)	30,8% (648)	100% (2104)
	Hard & Soft Science	60,76% (96)	39,24% (62)	100% (158)
Total		63,8% (2270)	36,2% (1288)	100% (3558)

Table 66: Field of Study * Gender: Crosstabulation; in orange: values above average, in blue: Values beyond average

Correlation

		Field of Study
Age	Correlation Coefficient (r_{pb})	,058**
	Sig. (2-tailed)	,002
	N	3558

Table 67: Correlation Field of Study and Age

Hypothesis Testing

Hypothesis 10: There are significant differences in information behaviour on SNS between students in the hard and the soft sciences.

A Kruskal-Wallis-Test did not provide any proof for hypothesis 10, which postulates that there are significant difference in information behaviour on SNS between students in the hard and the soft sciences. Therefore hypothesis 10 must be discarded.

The crosstabulation between the field of study and the degree of careful information behaviour illustrates this result explicitly. There are hardly any differences in the amount of respondents that show very careful, careful, careless, or very careless information behaviour whether they study hard sciences, soft sciences and the overall results for the whole sample size.

Field of Study * Careful Information Behaviour Crosstabulation

	Careful Information Behaviour				
	very careless	careless	careful	very careful	Total
Hard Science	11.57%	30.17%	30.17%	28.09%	100%
Soft Science	11.5%	29.56%	31.32%	27.61%	100%
Hard & Soft Science	8.86%	29.75%	28.48%	32.91%	100%
Total	11.41%	29.79%	30.78%	28.02%	100%

Table 68: Crosstabulation between Field of Study and careful Information Behaviour

Furthermore we tested if there are any significant differences in the intensitity of usage of SNS between students of the hard and the soft sciences. We conducted a Kruskal-Wallis, which resulted in the rejection of the null hypothesis (The distribution of the intensity of usage is the same across categories of the field of study). Therefore we can observe that students of the social sciences tend to show a slightly more intense usage behavior on SNS.

	Field of Study			
	Hard Science	Soft Science	Hard and Soft Science	Total
Light user	42,86%	54,2%	2,94%	
Moderate user	39,95%	55,68%	4,37%	
Normal user	34,44%	60,9%	4,66%	

Heavy user	30,42%	65,05%	4,53%	
Total	36,43%	59,13%	4,44%	100%

Table 69: Crosstabulation between Field of Study and Intensity of Usage; in orange: values above average, in blue: values beyond average

Hypothesis 11: A higher degree of privacy concerns is significantly positive correlated to a more careful information behaviour on SNS (intensity of reading the terms of use, degree of deactivation of advertising options, degree of activation of privacy mechanisms).

In order to assess this hypothesis it is necessary to clarify what "privacy concerns" means and how it can be operationalized:

4.5 Variable #5: Privacy Concerns

When testing for privacy concerns, attention must be drawn to the possibility of the correlation of privacy concerns with gender and age. For example, Aquisti and Gross (2006, 45) found that female respondents in general report statistically higher average concerns for privacy. Consequently, if hypothesis 11 were supported, women would also need to score higher in adopting a more careful information behaviour.

In a study about consumer's protection of online privacy and identity, Milne, Rohm and Bahl (2004) found out that "general attitudes and behaviours toward privacy were strong predictors of online privacy protection behaviour. A positive significant relationship was found for privacy concern (…) and active resistance" (Milne, Rohm, and Bahl 2004, 226). Similarly, Phelps, Nowak and Ferrell (2000) observed a strong relationship between the privacy concern level and beliefs in the importance of information protection among participants of their study about privacy concerns and consumers' willingness to provide personal information. Christofides et al. (2009, 343) argue that, although participants of their study disclosed a variety of personal and identifying information, "contrary to the assumption reports in the popular media, students in [their] survey were generally concerned about their privacy and reported that they were likely to use the variety of privacy settings" (Christofides, Muise, and Desmarais 2009, 343). Considering these results we hypothesize that a higher degree of privacy concerns is significantly positive correlated to a more careful information behaviour on SNS.

However, other studies have shown different results. In their study, "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook", Acquisti and Gross (2006) "detected little or no relation between participants' reported privacy attitudes and their likelihood of providing certain information" (Acquisti and Gross 2006, 50). They further suggest "that privacy attitudes have some effect on determining who joins the network, but after one has joined, there is very little marginal difference in information revelation across groups – which may be the result of perceived peer pressure or herding behavior" (Acquisti and Gross 2006, 50). But when looking further into that study, one can see that they only linked privacy concerns with the general provision of personal information such as birthday, address, schedule, and sexual or political orientation. However, without providing at least some of that information, using Facebook may not fulfil what they – in the same study – found out being the purpose of usage i.e. dating, self-promotion (and of course staying in touch with friends). More explicit they found that "respondents are fully aware that a social network is based on information sharing", which may be motivated by "revealing enough information (…) necessary/useful to me and other people to benefit from Facebook" (Acquisti and Gross 2006, 53).

Findings from Debatin (2009) support that the perceived benefits of social networking sites can "outweigh privacy concerns, even when concrete privacy invasion was experienced" (Debatin et al. 2009, 100).

So, in order to better assess this linkage one has to explore information behaviour in more detail – as we do (see section: "variable1: information behaviour"). Additionally, most authors solely investigated privacy concerns in the light of infringement attempts by individuals, but did not account for Facebook's own efforts to extract as much information as possible in order to sell it or use it for targeted advertising.

In order to conceptualize the variable "privacy concern" we used two existing indices that had already been proven valid many times (Harris and Westin 1990; 1991; 1994; 1995; 1996; Harris Interactive 2001a; 2001b; Zureik 2004; Kamaraguru and Cranor 2005; Gandy 2003; Smith, Milburg, and Burke 1996; Bellman et al. 2004; Malhotra, Kim, and Agarwal 2004). The first index is Westin's "Core Privacy Orientation Index", which is clearly interested in measuring the economic dimension of "consumer privacy" i.e. consumer's feelings about their privacy in the marketplace. Turow et al. (2009, 21) also used this index for measuring "American's confidence in the way business and the law handle information".

For constructing this index, survey participants were asked to indicate their agreement or disagreement with the following three statements (Harris Interactive 2001):

- *Consumers have lost all control over how personal information is collected and used by companies. (Q1)*
- *Most businesses handle the personal information they collect about consumers in a proper and confidential way. (Q2)*
- *Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today. (Q3)*

According to their answers, respondents were categorized into "Privacy Fundamentalists", "Privacy Unconcerned", and "Privacy Pragmatists".

Privacy Fundamentalists:

	Strongly Agree	Somewhat Agree	Somewhat Disagree	Strongly Disagree
Question 1	🟥	🟥		
Question 2			🟥	🟥

Question 3			🟥	🟥

Privacy Unconcerned:

	Strongly Agree	Somewhat Agree	Somewhat Disagree	Strongly Disagree
Question 1			🟥	🟥
Question 2	🟥	🟥		
Question 3	🟥	🟥		

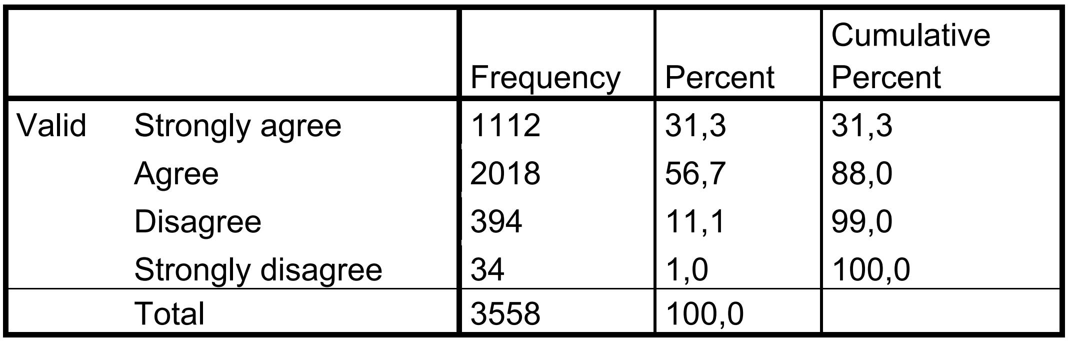
Privacy Pragmatists:

>> Every other possible combination of answers.

	Strongly Agree	Somewhat Agree	Somewhat Disagree	Strongly Disagree
Question 1	▨	▨	▨	▨
Question 2	▨	▨	▨	▨
Question 3	▨	▨	▨	▨

The following section illustrates for each of the three statements from the Westin Index the distribution of answers. It shows that especially when it comes to the first statement, that consumers have lost all control over how personal information is collected and used by companies, a large majority (together 88%) agrees (56.7%) or even strongly agrees (31.3%). For the second statement, that most businesses handle personal information that they collect about consumers in a proper and confidential way, also more than half of the respondents (54.9%) disagreed and showed themselves concerned. However, 36.4% did agree, which is more than a third who feel comfortable with the way businesses treat their personal data. In contrast, only 18.8% of the respondents felt that existing laws and organizational practices provide a reasonable level of protection for consumer privacy today. The remaining 81.2% seems to feel concerned about the level of protection granted by the state.

Q49: Consumers have lost all control over how personal information is collected and used by companies.



		Frequency	Percent	Cumulative Percent
Valid	Strongly agree	1112	31,3	31,3
	Agree	2018	56,7	88,0
	Disagree	394	11,1	99,0
	Strongly disagree	34	1,0	100,0
	Total	3558	100,0	

Table 70: Results to Question 49

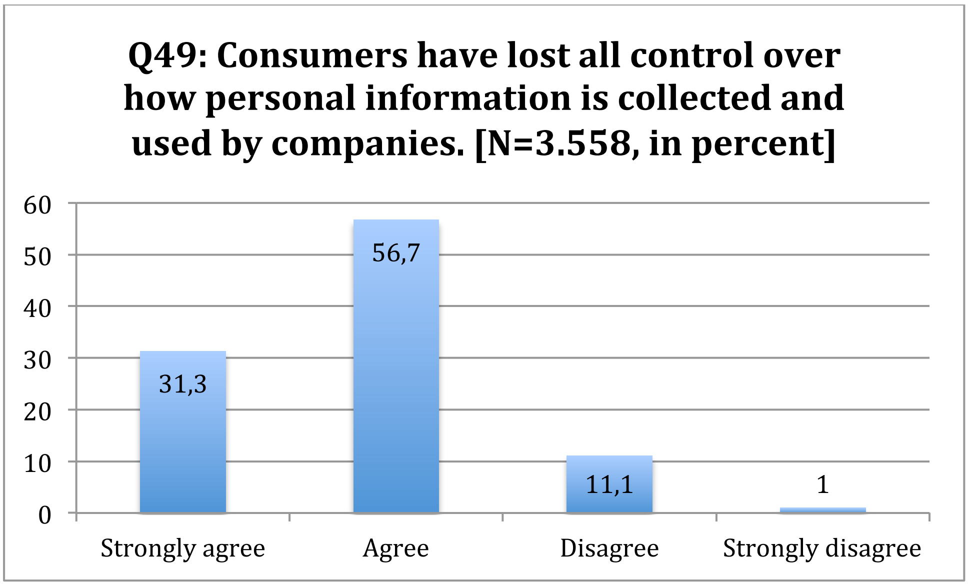


Figure 55: Results to Question 49

Q50: Most businesses handle the personal information they collect about consumers in a proper and confidential way.

		Frequency	Percent	Cumulative Percent
Valid	Strongly agree	42	1,2	1,2
	Agree	1295	36,4	37,6
	Disagree	1952	54,9	92,4
	Strongly disagree	269	7,6	100,0
	Total	3558	100,0	

Table 71: Results to Question 50

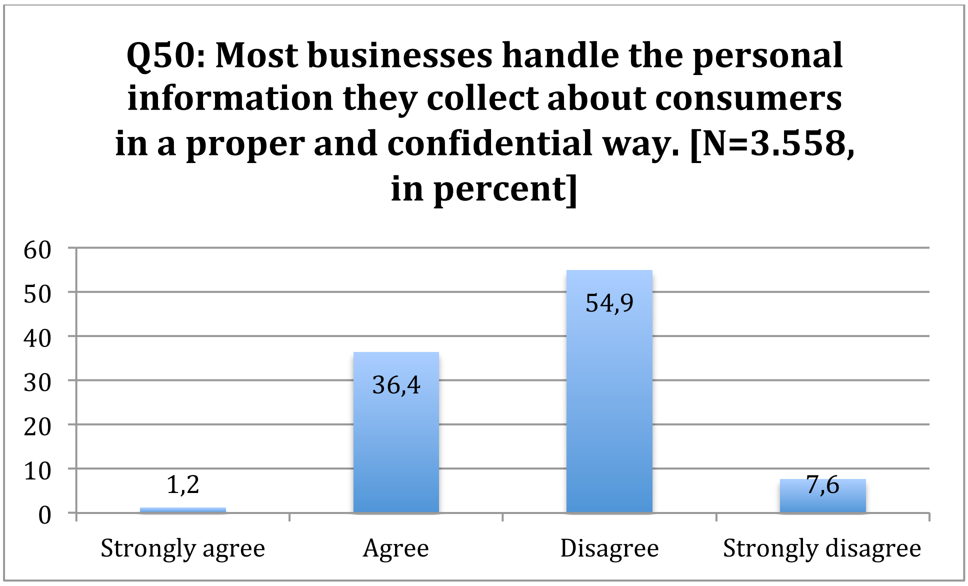


Figure 56: Results to Question 50

<u>Q51: Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.</u>

		Frequency	Percent	Cumulative Percent
Valid	Strongly agree	12	,3	,3
	Agree	658	18,5	18,8
	Disagree	2373	66,7	85,5
	Strongly disagree	515	14,5	100,0
	Total	3558	100,0	

Table 72: Results to Question 51

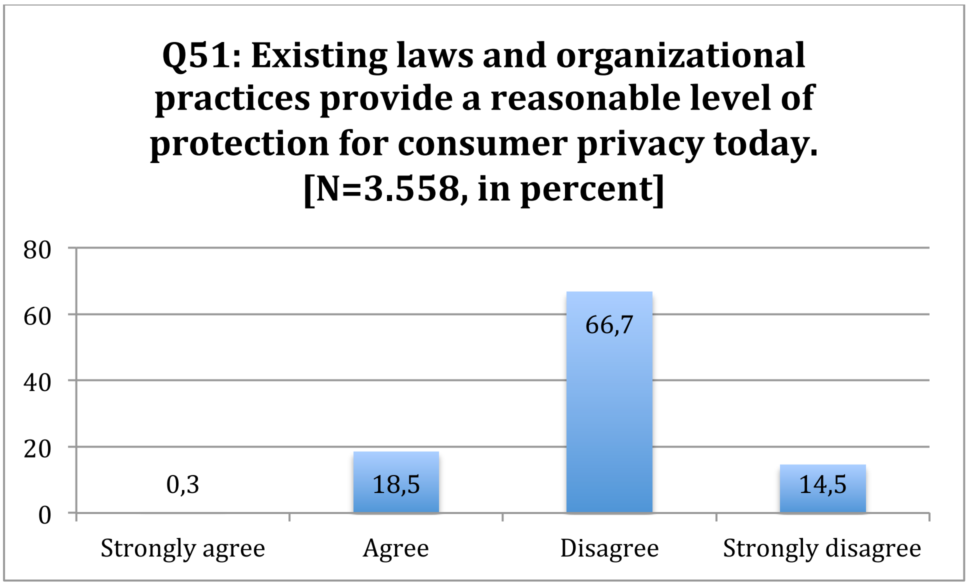


Figure 57: Results to Question 51

4.5.1 Privacy Concern Index - Part 1 (Westin/Harris)

Putting all these result together and constructing the three categories "privacy concerned", "privacy pragmatists", and "privacy unconcerned" as it is done in the Westin Core Privacy Orientation Index, we received the results as shown in the figure and table below. We decided to change the label of the category "privacy fundamentalists" into the category of "privacy concerned", since we feel that fundamentalist is a strongly normative label, that somewhat suggests that respondents, that fall into this category are overly protective (i.e. fundamental) about their privacy. In our point of view the term "privacy concerned" is more neutral and therefore fits better. Over half of our respondents (53%) therefore class among the category of the "privacy concerned", 43.8% rank among the "privacy pragmatists", and only 3.2% are unconcerned when it comes to their privacy.

Privacy Concern Index 1

		Frequency	Percent	Cumulative Percent
Valid	Concerned	1884	53,0	53,0
	Pragmatists	1560	43,8	96,8
	Unconcerned	114	3,2	100,0
	Total	3558	100,0	

Table 73: Distribution Privacy Concern Index Pt.1

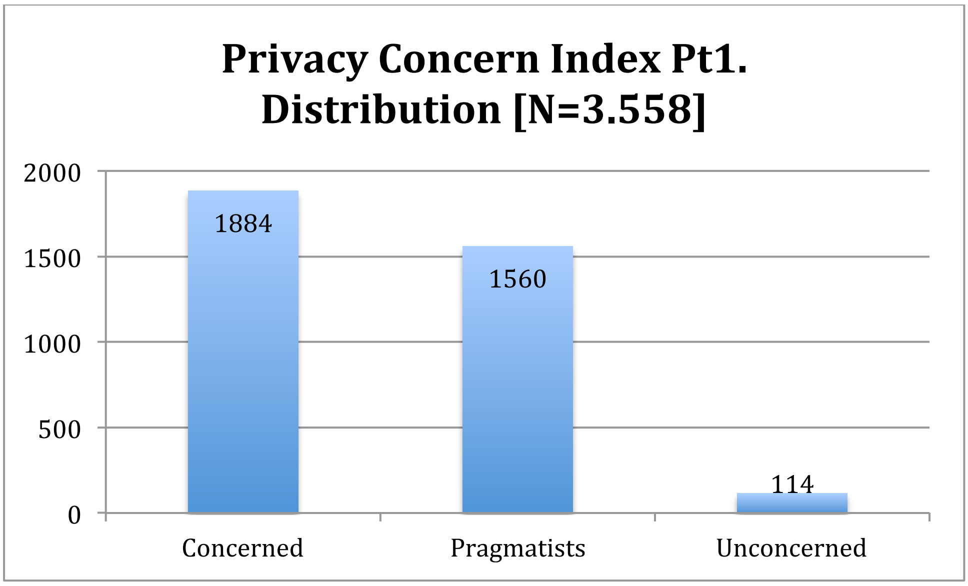


Figure 58: Distribution Privacy Concern Index Pt. 1(Frequency)

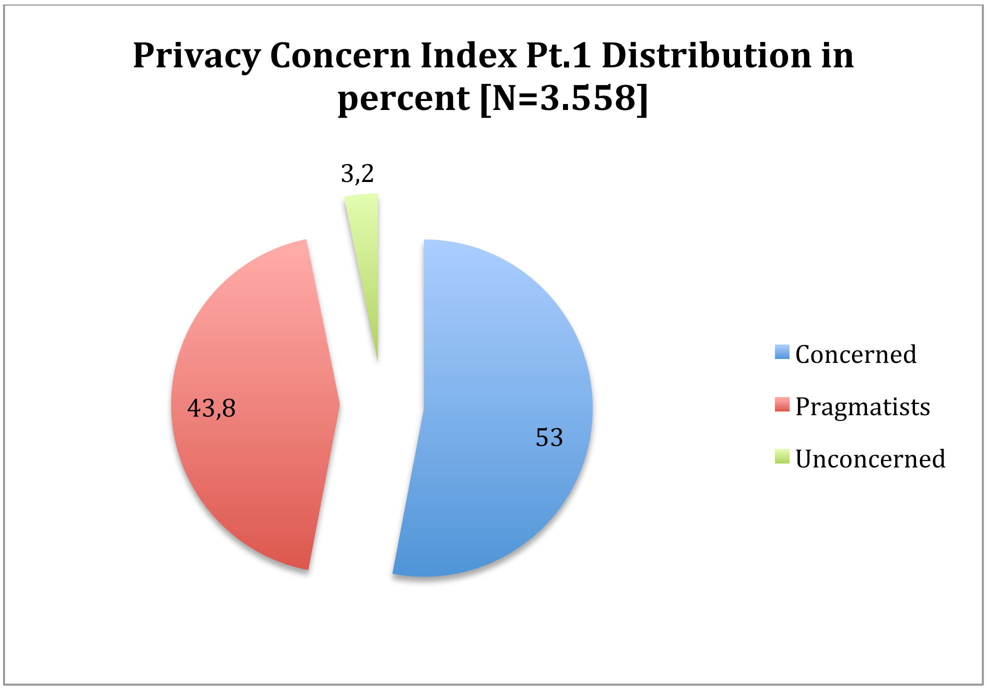


Figure 59: Distribution Privacy Concern Index Pt.1 (Percentage)

4.5.2 Privacy Concern Index - Part 2 (Online Information Privacy Concern)

The second scale we used in our survey was developed by Smith et al. (1996) and aims at measuring "Online Informational Privacy Concern". This index is widely used and adapted and proven valid as well. See for example Bellman et al. 2004; Malhotra, Kim, and Agarwal 2004.

In this index four sub-categories are distinguished:

- Data Collection,
- Improper Access,
- Errors,
- Unauthorized Secondary Use.

For each category we chose one question from the original questionnaire (we have slightly modified some questions by including e.g. "companies and websites, such as Social Networking Sites". The modification are listed in the section below, where each statement is analysed)

- *When Websites ask me for personal information, I sometimes think twice before providing it. (Collection)*
- *Websites should devote more time and effort to preventing illegal access to personal information (Improper access).*
- *All the information received on Websites should be double-checked for accuracy – no matter how much this costs (Errors).*
- *Websites should never sell the personal information they have collected to other Websites. (unauthorized secondary use).*

Survey participants were asked to indicate their agreement or disagreement on a seven-point likert scale, with 7 meaning "strongly agree" and 1 meaning "strongly disagree". The single results were added up, resulting in a possible range of 4 to 28 points. Based on the Westin Index, three categories were introduced:

28 – 21	*Privacy Concerned*
20 – 13	*Privacy Pragmatists*
12 - 4	*Privacy Unconcerned*

In the following we illustrate for each of the four statements from the *Online Informational Privacy Concern* Index the distribution of answers, as well as a comparison between the level of agreement. It clearly shows that respondents' agreement to the statements "When Websites ask me for personal information, I sometimes think twice before providing it." (Q52) and "Companies and Websites, such as Social Networking Sites, should devote more time and effort for preventing illegal access to personal information." (Q53) is very similar. A majority of the students in our survey agreed to some extent with these statements. For Q55 respondents agreed even more strongly with the presented statement that companies and Websites, such as Social Networking Sites, should never sell the personal information they have collected to other companies or Websites. Only for Q54 ("Internet companies should make sure that all personal information they have collected and stored about their customers, is true and accurate – no matter how much this costs") answers were more evenly distributed – with around 24% neither agreeing nor disagreeing, around 20% disagreeing to some extent, and around 20% for each category of agreement (slightly agree, agree, strongly agree).

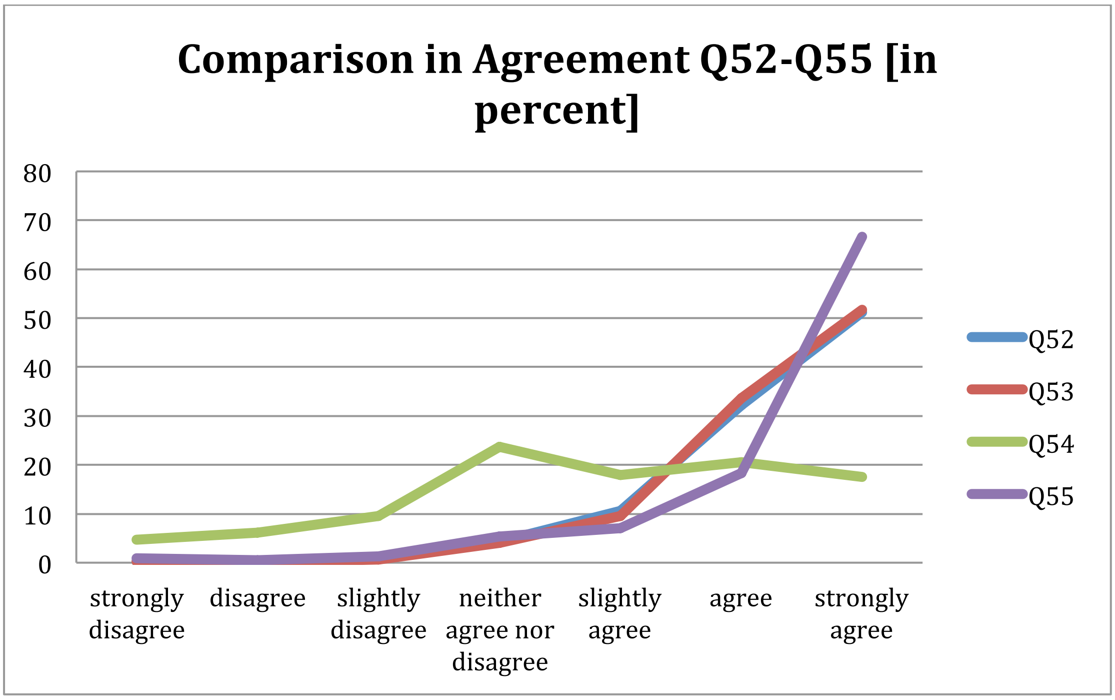


Figure 60: Comparison in Agreement Q52-Q55

The following tables and charts show the detailed results for all four statements of the *Online Informational Privacy Concern Index.*

Q52: When Websites ask me for personal information, I sometimes think twice before providing it. (Collection)

		Frequency	Percent	Cumulative Percent
Valid	strongly disagree	6	,2	,2
	disagree	12	,3	,5
	slightly disagree	42	1,2	1,7
	neither agree nor disagree	154	4,3	6,0

	slightly agree	376	10,6	16,6
	agree	1146	32,2	48,8
	strongly agree	1822	51,2	100,0
	Total	3558	100,0	

Table 74: Results to Question 52

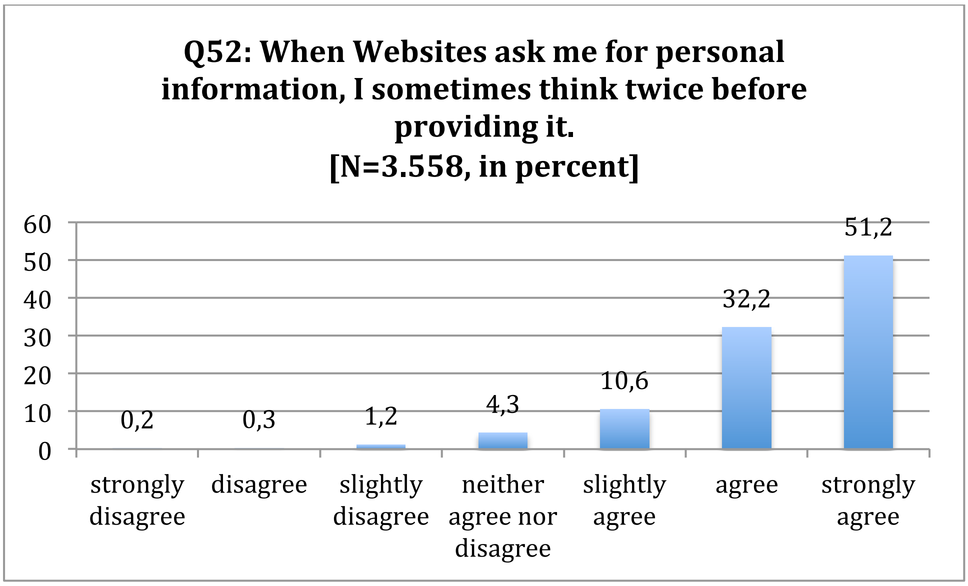


Figure 61: Results to Question 52

Q53:* Companies and Websites, such as Social Networking Sites, should devote more time and effort for preventing illegal access to personal information. *(Improper access).

		Frequency	Percent	Cumulative Percent
Valid	strongly disagree	8	,2	,2
	disagree	3	,1	,3
	slightly disagree	26	,7	1,0
	neither agree nor disagree	144	4,0	5,1
	slightly agree	340	9,6	14,6
	agree	1196	33,6	48,3
	strongly agree	1841	51,7	100,0
	Total	3558	100,0	

Table 75: Results to Question 53

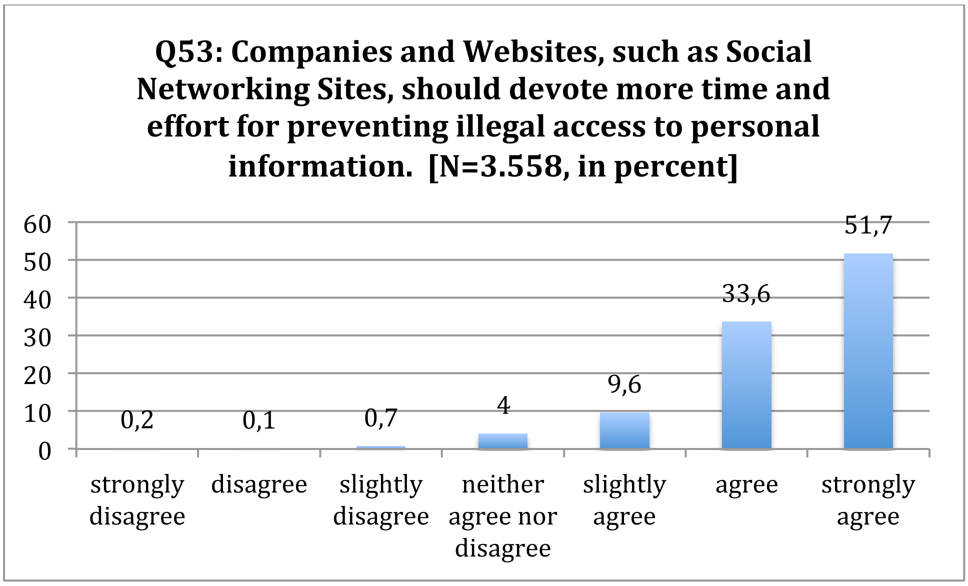


Figure 62: Results to Question 53

Q54: Internet companies should make sure that all personal information they have collected and stored about their customers is true and accurate – no matter how much this costs. *(Errors).*

		Frequency	Percent	Cumulative Percent
Valid	strongly disagree	166	4,7	4,7
	disagree	218	6,1	10,8
	slightly disagree	342	9,6	20,4
	neither agree nor disagree	843	23,7	44,1
	slightly agree	636	17,9	62,0
	agree	731	20,5	82,5
	strongly agree	622	17,5	100,0
	Total	3558	100,0	

Table 76: Results to Question 54

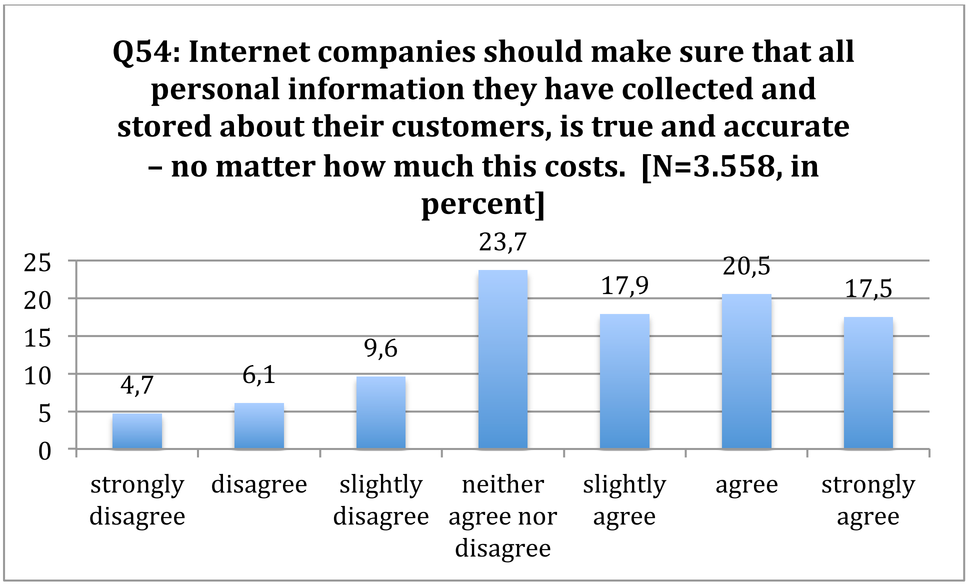


Figure 63: Results to Question 54

Q55: Companies and Websites, such as Social Networking Sites, should never sell the personal information they have collected to other companies or Websites. *(Unauthorized secondary use).*

		Frequency	Percent	Cumulative Percent
Valid	strongly disagree	31	,9	,9
	disagree	18	,5	1,4
	slightly disagree	47	1,3	2,7
	neither agree nor disagree	188	5,3	8,0
	slightly agree	250	7,0	15,0
	agree	650	18,3	33,3
	strongly agree	2374	66,7	100,0
	Total	3558	100,0	

Table 77: Results to Question 55

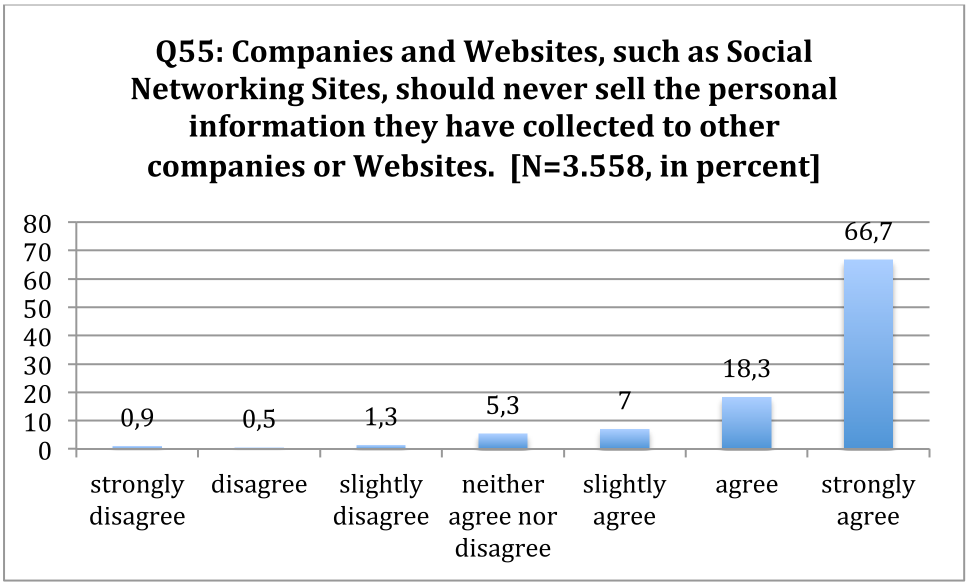


Figure 64: Results to Question 55

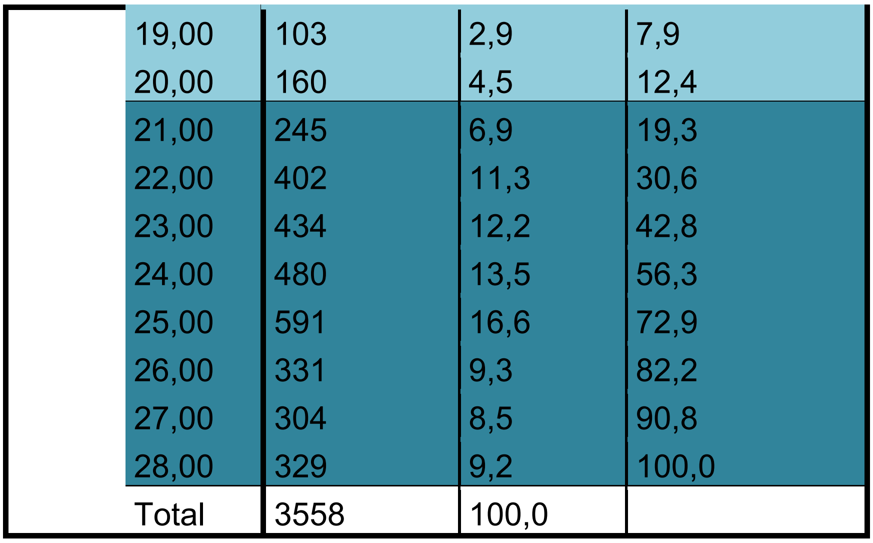
For calculating the Online Informational Privacy Concern Index we added up the single results, resulting in a possible range of 4 to 28 points. Based on the Westin Index, three categories were introduced:

28 – 21	*Privacy Concerned*
20 - 13	*Privacy Pragmatists*
12 - 4	*Privacy Unconcerned*

The single results on that score are shown in the following table. The different categories of privacy concern are marked with different colours.

Privacy Concern Index Pt.2

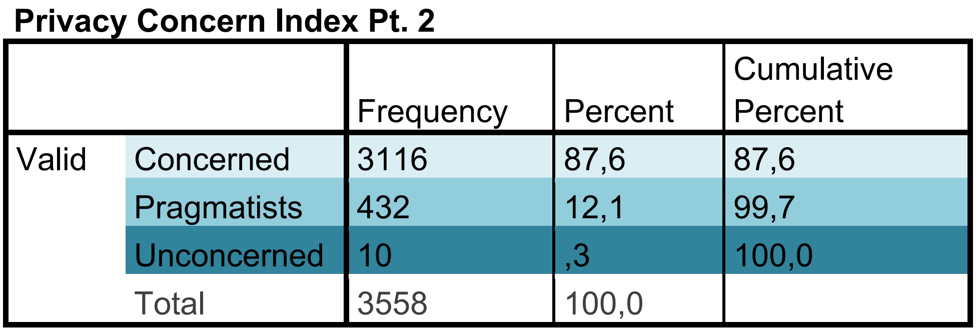
		Frequency	Percent	Cumulative Percent
Valid	4,00	2	,1	,1
	10,00	2	,1	,1
	11,00	1	,0	,1
	12,00	5	,1	,3
	13,00	6	,2	,4
	14,00	6	,2	,6
	15,00	11	,3	,9
	16,00	46	1,3	2,2
	17,00	50	1,4	3,6
	18,00	50	1,4	5,0



	19,00	103	2,9	7,9
	20,00	160	4,5	12,4
	21,00	245	6,9	19,3
	22,00	402	11,3	30,6
	23,00	434	12,2	42,8
	24,00	480	13,5	56,3
	25,00	591	16,6	72,9
	26,00	331	9,3	82,2
	27,00	304	8,5	90,8
	28,00	329	9,2	100,0
	Total	3558	100,0	

Table 78: Distribution Privacy Concern Index Pt. 2 – Results for each score

Putting all these result together and constructing the three categories "privacy concerned", "privacy pragmatists", and "privacy unconcerned" for the realm of the Internet, we got the results shown in the figure and table below. A majority of our respondents (87.6%) therefore class among the category of the "privacy concerned", 12.1% rank among the "privacy pragmatists", and only 0.3% are unconcerned when it comes to their privacy online.



Privacy Concern Index Pt. 2

		Frequency	Percent	Cumulative Percent
Valid	Concerned	3116	87,6	87,6
	Pragmatists	432	12,1	99,7
	Unconcerned	10	,3	100,0
	Total	3558	100,0	

Table 79: Distribution Privacy Concern Index Pt. 2

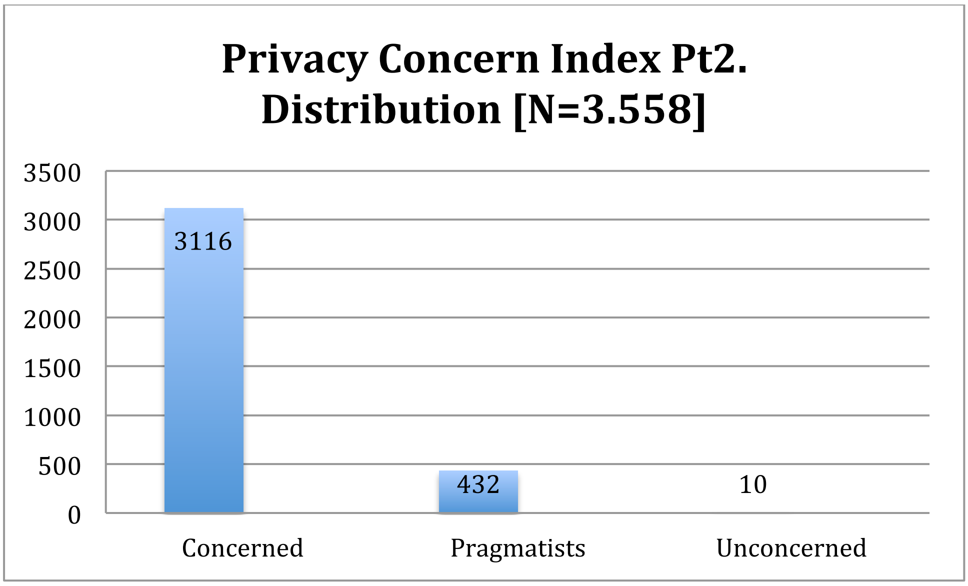


Figure 65: Distribution Privacy Concern Index Pt.2 (Frequency)

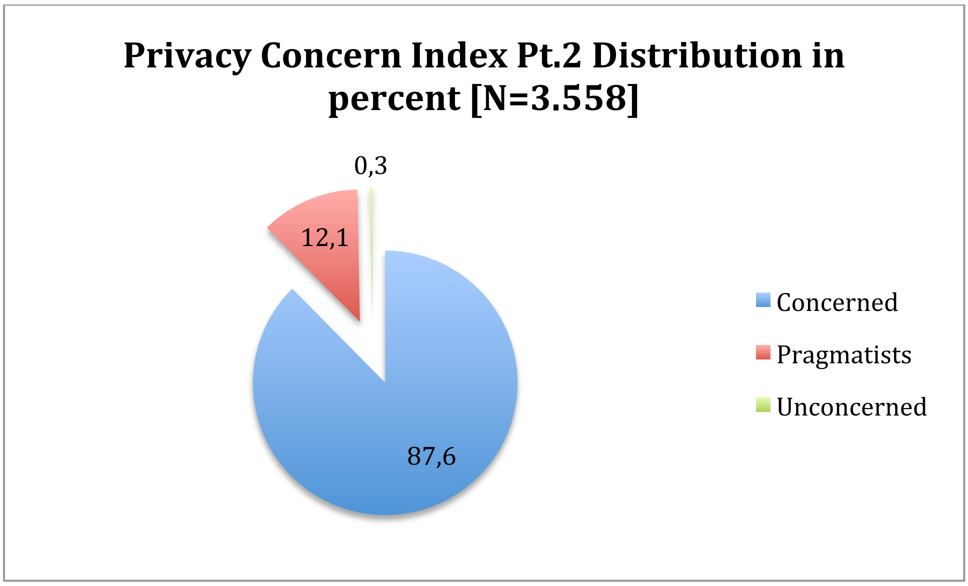


Figure 66: Distribution Privacy Concern Index Pt. 2 (Percentage)

4.5.3 Privacy Concern Index - Combination of the Two Indices:

In order to get one Index that accounts as well for Westin's categories as for the specific online environment social media is located in, we have combined these two Indices.

Therefore we analysed the single results for the two indices and received the following results:

		Index pt.1 (Westin/Harris "Core Privacy Orientation Index")		
		Concerned	Pragmatists	Unconcerned
Index pt.2 ("Online Informational Privacy Concern Index")	Concerned	47.7%	37.7%	2.2%
	Pragmatists	5.0%	6.0%	1.0%
	Unconcerned	0.2%	0.2%	0.0%

Table 80: Combination Privacy Concern Index Pt1 and Pt. 2

The table above shows that 47.7% of the respondents are “privacy concerned” according to both indices, 6.0% are categorized “privacy pragmatists” in both indices, and no respondents at all scored the category of “privacy unconcerned” in the Westin/Harris “Core Privacy Orientation Index” and the “Online Informational Privacy Concern Index” at the same time.

37.7% and 5.0% of the respondents were labelled “concerned” in the one, and “pragmatists” in the other index. Combining these two parts, 42.7% of the respondents were at least in one of the two indices considered “privacy concerned”, and scored “privacy pragmatists” in the other. This huge part of respondents can be classified as “rather privacy concerned”, since they definitely tend to be more concerned than those that scored “pragmatists” in both indices, but tend to be less concerned than those that scored “concerned” in both indices. The same applies for respondents that scored in one index “pragmatists”, while got categorized as “unconcerned” in the other index. For these respondents we introduced the category of “rather privacy unconcerned”.

A remaining 2.4 % of the 3558 respondents showed very mixed results: their results indicated them as “privacy concerned” in the one index, while in the other index they scored “privacy unconcerned”. Respondents who showed this kind of answering scheme were categorized as “privacy pragmatists”, and added to the existing 6.0% already considered “pragmatists”.

Therefore combining these two indices, we got the following results:

Privacy Concern Index

	Frequency	Percent	Cumulative Percent
Concerned	1697	47,7	47,7
Rather Concerned	1520	42,7	90,4
Pragmatists	300	8,4	98,8
Rather Unconcerned	41	1,2	100,0
Unconcerned	0	0	100,0
Total	3558	100,0	

Table 81: Results Privacy Concern Index

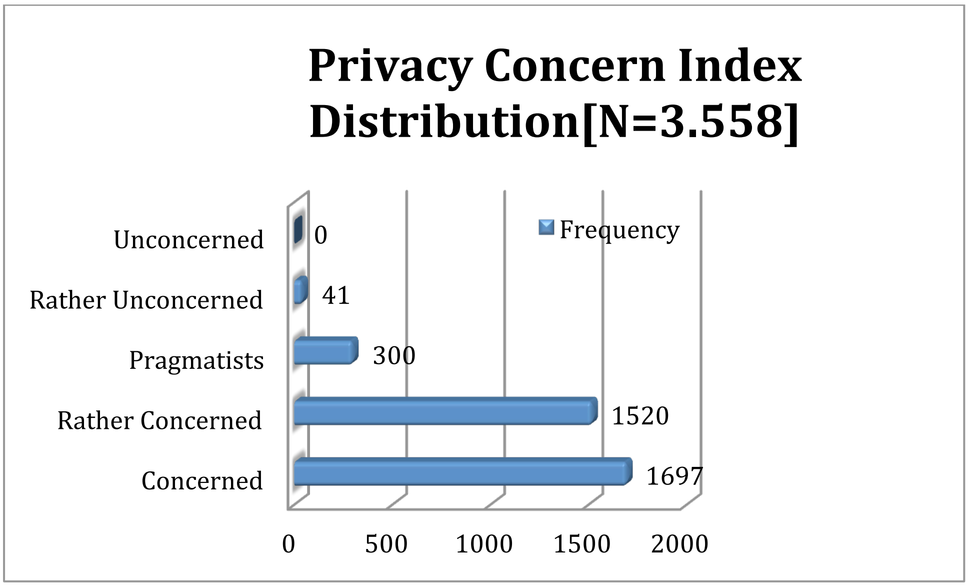


Figure 67: Distribution Privacy Concern Index (Frequency)

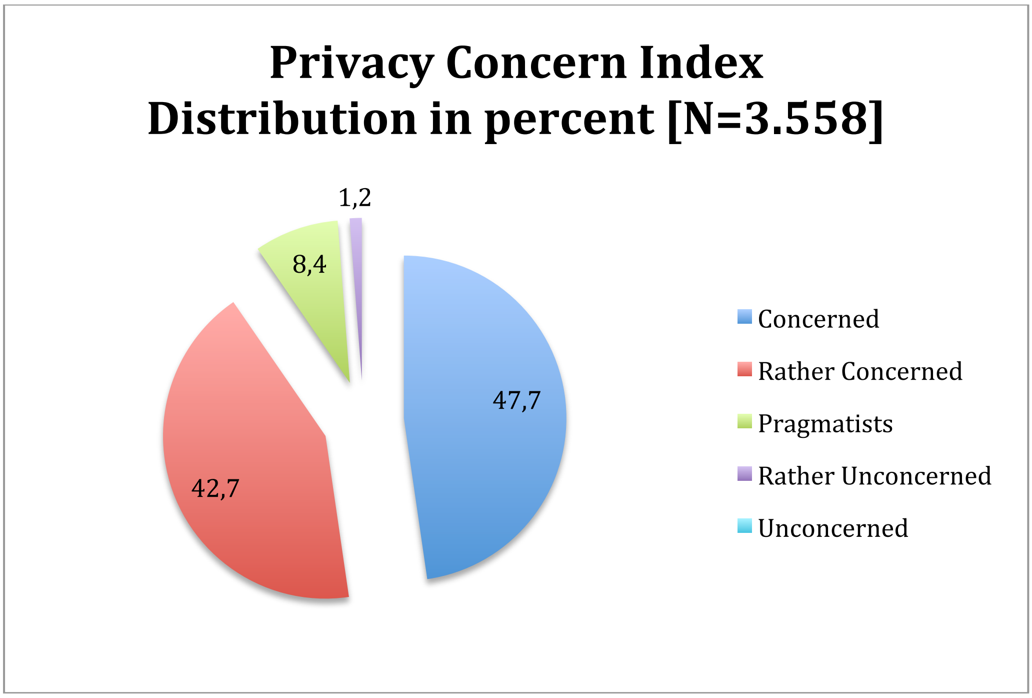


Figure 68: Distribution Privacy Concern Index (Percentage)

4.5.4 Correlations:

Conducting a correlation analysis, we found no significant associations between the results of the privacy concern index and any demographic variables. There was also no significant relationship between privacy concerns and the intensity of the usage behaviour.

But a Spearman's Rank Order analysis showed considerable correlation between the Privacy Concern Index, the Surveillance Attitude Index and the Surveillance Knowledge Index.

Especially between the Privacy Concern Index and the Surveillance Attitude Index a statistically significant correlation exists with a Spearman's rho of -0.191. This implies that respondents who are more critical of surveillance also tended to be more concerned about their privacy. The same is true for the Surveillance Knowledge Index, which showed a correlation coefficient of 0.094 with the Privacy Concern Index, indicating that respondents that scored lower values on the Surveillance Knowledge Index (i.e. have higher knowledge) also scored lower on the Privacy Concern Index (i.e. are more concerned).

Additionally, results showed a weak association between the Surveillance Attitude Index and the Surveillance Knowledge Index. With a Spearman's rho of -0.094 these two indices are significantly negative correlated, meaning that higher knowledge correlates with a more critical attitude towards surveillance.

The table below shows the results from the correlation analysis for these indices:

Correlations

		Privacy Concern Index	Surveillance Attitude Index	Surveillance Knowledge Index
Privacy Concern Index	Correlation Coefficient (Spearman's Rho)	1,000	-,191**	,094**
	Sig. (2-tailed)	.	,000	,000
	N	3558	3558	3558
Surveillance Attitude Index	Correlation Coefficient (Spearman's Rho)	-,191**	1,000	-,094**
	Sig. (2-tailed)	,000	.	,000
	N	3558	3558	3558

Surveillance Knowledge Index	Correlation Coefficient (Spearman's Rho)	,094**	-,094**	1,000
	Sig. (2-tailed)	,000	,000	.
	N	3558	3558	3558

**. Correlation is significant at the 0.01 level (2-tailed).

Table 82: Correlation of different Indices

Hypothesis 11: A higher degree of privacy concerns is significantly positive correlated to a more careful information behaviour on SNS (intensity of reading the terms of use, degree of deactivation of advertising options, degree of activation of privacy mechanisms).

A Spearman's Rank Order correlation was run to determine the relationship between the Privacy Concern Index and the Carefulness Index. Our findings show that there is a minor, but significant negative correlation with a Spearman's rho of -.078. Since scoring low on the privacy concern index indicates a more concerned attitude, whereas scoring high on the carefulness index indicates a more careful information behaviour, this negative correlation validates hypothesis 11.

Careful Information Behaviour * Privacy Concern Index Correlations

		Carefulness Index	Privacy Concern Index
Carefulness Index	Correlation Coefficient (Spearman's Rho)	1,000	-,078**
	Sig. (2-tailed)	.	,000
	N	3558	3558

**. Correlation is significant at the 0.01 level (2-tailed).

Table 83: Correlation Privacy Concern Index with Careful Information Behaviour

Additionally we conducted a Spearman's Correlation with the original two parts of the combined Privacy Concern Index. Correlation results for Part 1 and Part 2 are similar to the combined Privacy Concern Index, and show a somewhat minor , but significant negative correlation.

		Privacy Concern Index Pt.2	Privacy Concern Index Pt.1
Carefulness Index	Correlation Coefficient	-,071**	-,058**
	Sig. (2-tailed)	,000	,001

	N	3558	3558

****. Correlation is significant at the 0.01 level (2-tailed).**

Table 84: Correlation Carefulness Index with Privacy Concern Index Pt.1 and Pt.2

4.6 Additional: Targeted Advertising

As part of our study we wanted to find out how large students' knowledge of surveillance is in general, which attitudes they have towards surveillance and privacy, how much knowledge they have about concrete social networking sites and their individual information behaviour in context of those social networking sites. But additionally to that, we paid special attention to targeted advertising. How much students know about it, what is their attitude towards it and what are their concerns, and how do they actually behave in context of targeted advertising.

4.6.1 Knowledge

In order to test students' knowledge about advertising on Facebook, we asked them if the presented statement was true or false. Also, an "I don't know"-answering category was provided.

A clear majority of 83.2% was aware that the statement "On Facebook all users see the same advertisements" (Q41) is false.

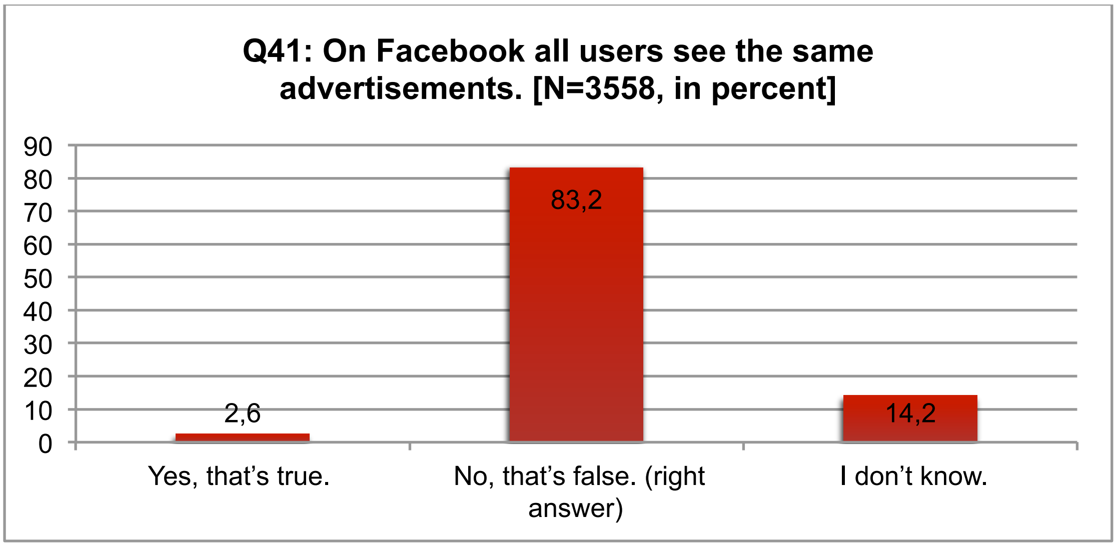


Figure 69: Results to Question 41

When asked, if it is true that Facebook is allowed to give personal data (e.g. contact information, interests, activities, friends, online behaviour) to third parties/other companies for advertising purposes, respondents were not sure about their answers. 31.8% checked "I don't know", another third (32.6%) thought it was correct (which is actually the right answer), and a very small majority of 35.6% answered with " No, that's false".

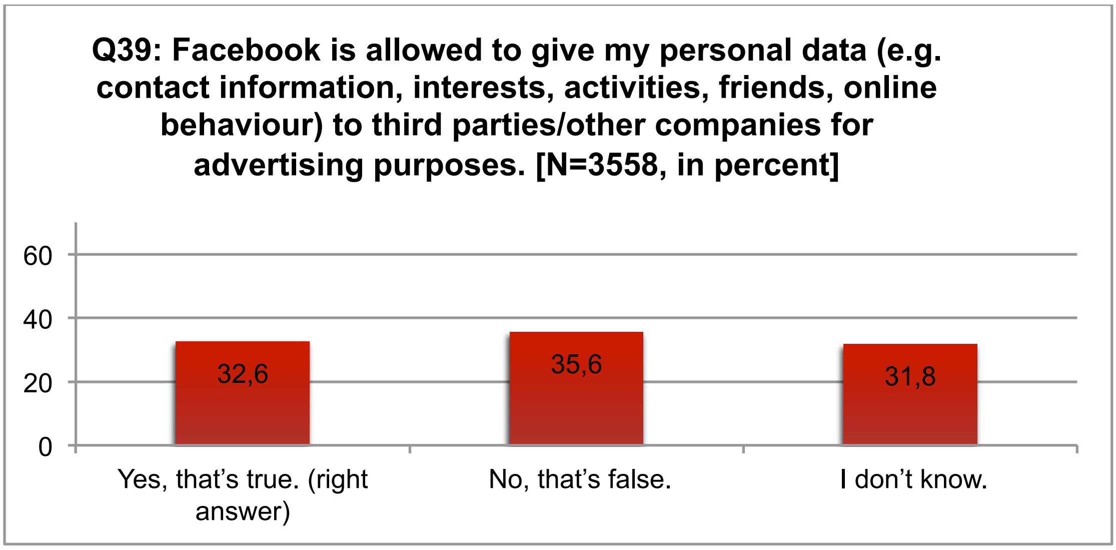


Figure 70: Results to Question 39

Huge uncertainty also determined the answers to the question if advertisements, commercial sites and paid services on social networking sites, such as Facebook, must be marked as such. Only 19.4% knew the correct answer (No, that's false), 46.5% gave the wrong answer, and 34.1% of the respondents said that they don't know the answer.

["You understand that we may not always identify paid services and communications as such." (Facebook - Terms)]

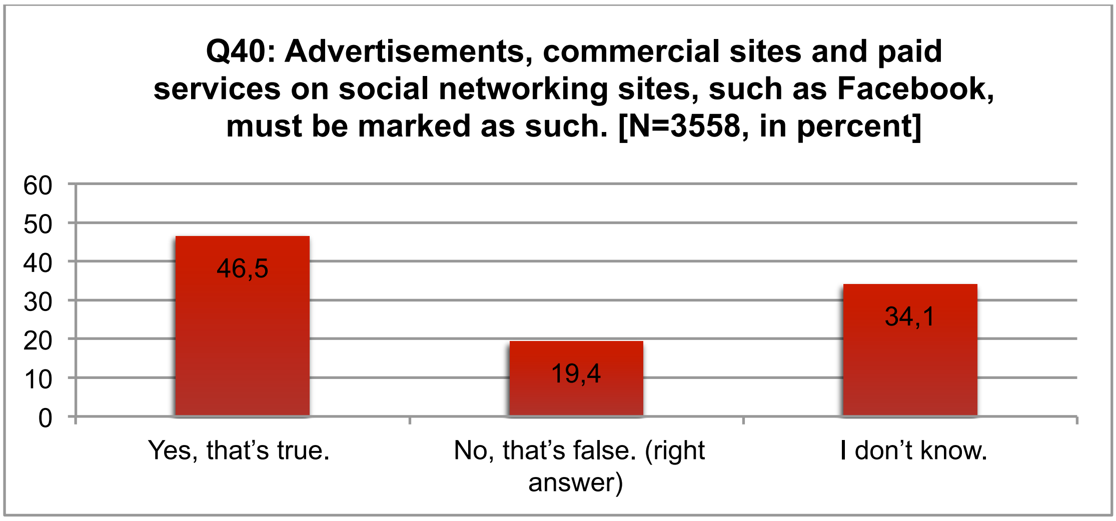


Figure 71: Results to Question 40

Correlations

We conducted Chi-Square Tests and calculated the phi coefficients for each item in order to determine if there is a significant association between respondent's knowledge about targeted advertising and gender. We created contingency tables for better display. We found a weak association between gender and knowledge about advertising on Facebook (i.e. male respondents and correct answers are positively correlated). This association was most distinctive for Question 39 (also see the crosstabulation below).

Symmetric Measures

		Value	Approx. Sig.
Q39	Phi	,150	,000
Q40	Phi	,080	,000
Q41	Phi	,073	,000
N of Valid Cases		3558	

Table 85: Phi Values for Q39, Q40, Q41 and gender.
Q39: FB is allowed to give my personal data (e.g. contact information, interests, activities, friends, online behaviour) to third parties/other companies for advertising purposes
Q40: Advertisements, commercial sites and paid services on social networking sites, such as Facebook, must be marked as such.
Q41: On Facebook all users see the same advertisements.

Gender * Q39 Crosstabulation

		Question 39		
		Not the right answer	Right Answer	Total
	female	1650	620	2270
		72,7%	27,3%	100,0%
	male	748	540	1288
		58,1%	41,9%	100,0%
Total		2398	1160	3558
		67,4%	32,6%	100,0%

Table 86: Crosstabulation between Gender and Q39 (FB is allowed to give my personal data (e.g. contact information, interests, activities, friends, online behaviour) to third parties/other companies for advertising purposes); in orange: values above average, in blue: values below average.

For other demographic variables, such as age, level of study and average monthly income we did not find any correlation (except for a weak one between Q39 and income, contingency coefficient = 0,08).

4.6.2 Attitude/Concerns

Asked if they actually want websites to tailor ads to personal interests, an overwhelming majority opposed this practice.

Judging from these results it is even more questionable why there is no opt-out possibility on Facebook. Or in other terms: these results make it very clear why FB – from a profit-oriented point of view – has no interest in offering such an option.

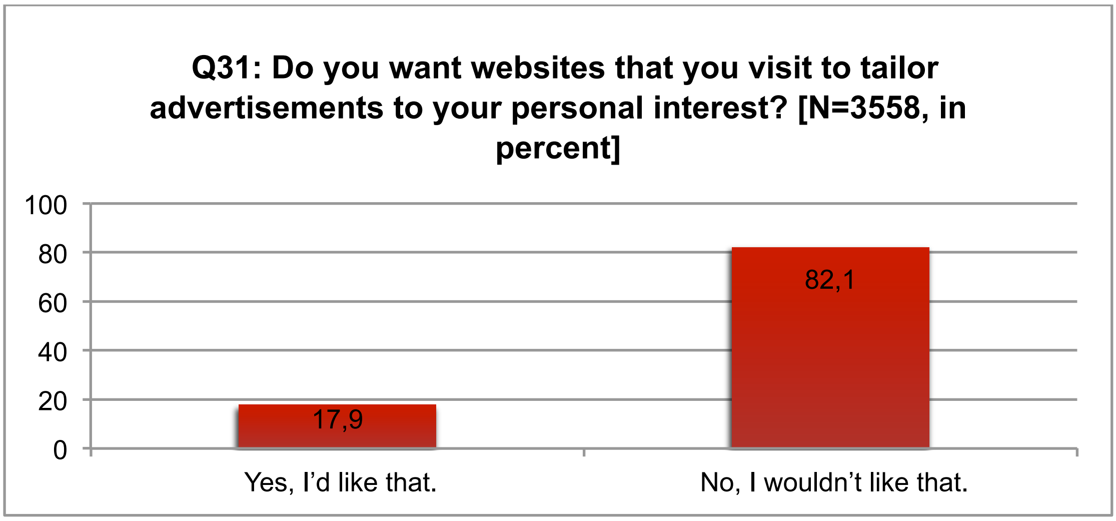


Figure 72: Results to Question 31

A correlation analysis was run to determine the relationship between respondents' attitude towards targeted advertising and the surveillance critique index. We found significantly positive correlation with a value of .187, meaning that answering "no, I wouldn't like websites to tailor advertisements to my personal interests" is positively related to a more critical attitude towards surveillance.

Attitude towards Targeted Advertising * Surveillance Critique Index Correlations

		Attitude towards Targeted Advertising (Q31)	Surveillance Critique Index
Attitude towards Targeted Advertising (Q31)	Correlation Coefficient (r_{pb})	1,000	,196**
	Sig. (2-tailed)	.	,000
	N	3558	3558
Surveillance Critique	Pearson Correlation	,196**	1,000

Index	Sig. (2-tailed)	,000	.
	N	3558	3558

**. Correlation is significant at the 0.01 level (2-tailed).

Table 87: Correlation Attitude towards Targeted Advertising with Surveillance Critique Index

We also conducted a Chi Square Test and crosstabulation, and calculated Phi values in order to analyse if there is any statistically significant association between users attitude towards advertising and all the other indices. Results indicate that there is a positive relation between users who are critical of targeted advertising and a more careful information behaviour (C = 0.092), between users who are critical of targeted advertising and a less intense usage behaviour (C = 0.123) and there is also a significant positive relationship between respondents who are more concerned about their privacy and respondents who are against targeted advertising (C = 0.112)

Correlation analysis with other demographic variables showed only an association with gender (Phi -0,097).

Table 50 illustrates that in relation more male respondents are in favour of tailored advertisements: whereas only 15.1% of all female respondents answered that they would like advertisements to be tailored to their personal interests, it were 22.8% of all male respondents who did so.

Crosstabulation

		Do you want websites that you visit to tailor advertisements to your personal interest?		
		Yes, I'd like that.	No, I wouldn't like that	Total
Gender	female	15.11%	84.89%	100%
	male	22.83%	77.17%	100%
Total		17.9%	82.1%	100%

Table 88: Crosstabulation Attitude towards Targeted Advertising with Gender

Another example for users concerns about targeted advertising is their distinct rejection of advertisements that are tailored based on location data. A huge majority of 71% stated their disapproval to such advertising practice.

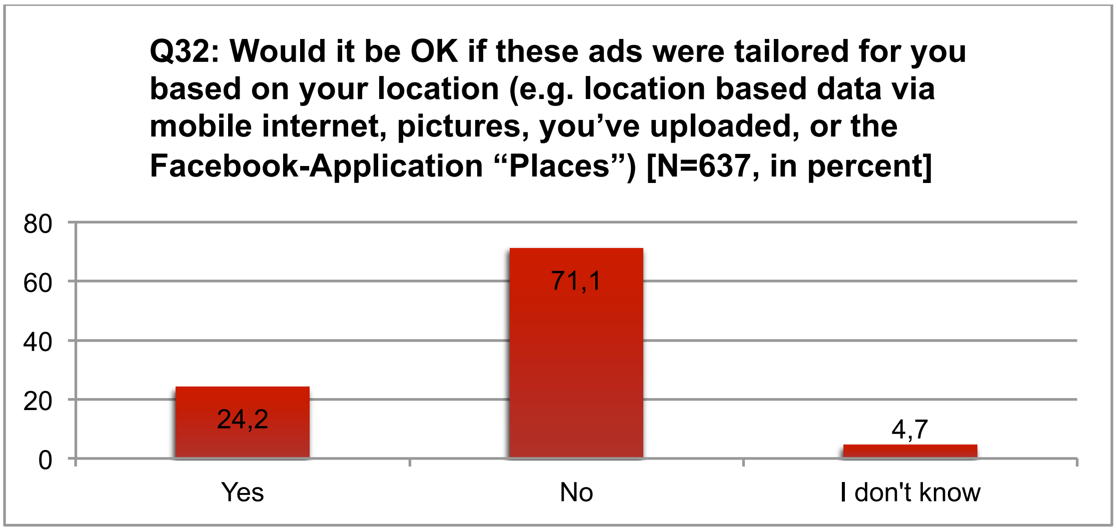


Figure 73: Results to Question 32

4.6.3 Behaviour

It is often questioned, if people actually read targeted ads, like those displayed on the right side of your Facebook Profile. Our results show that though a majority never or hardly ever read these ads, 23.1% do read them at least once a month (or even more often) after all. But only 22% of the respondents have actually ever clicked on any ads. However, keeping in mind that Facebook has around 900mio. users, 22% is quite a lot.

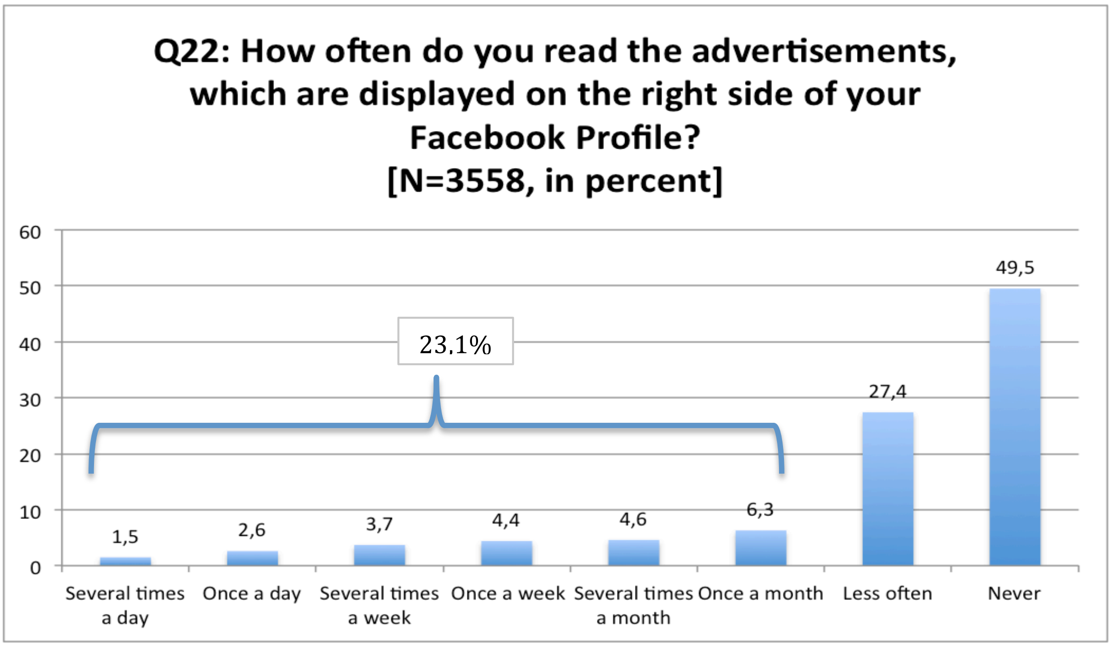


Figure 74: Results to Question 22

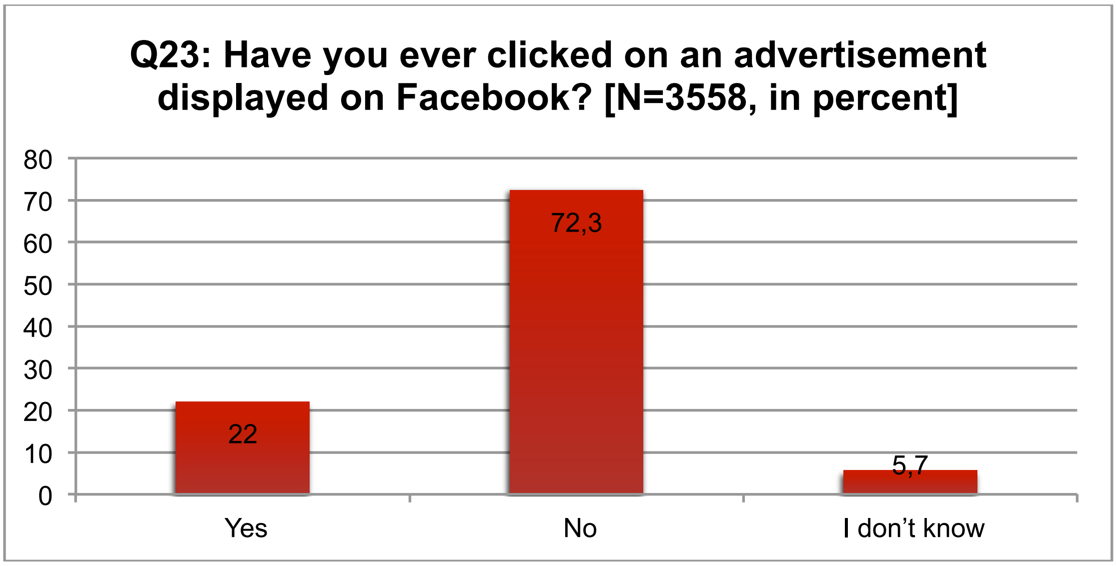


Figure 75: Results to Question 23

How much value targeted advertising methods actually have for Facebook becomes even more obvious, when taking into account the results of another question we asked the study participants: "Have you ever joined a group or site, that has been established and is run by a commercial actor (e.g. local restaurants or shopping malls, brand communities such as Starbucks, Nike, etc…)?".

Brand sites are the really successful marketing strategies on social media. They aim at establishing deep and long-lasting relationships and an intensified and ubiquitous brand presence in the lives of customers (Illobre 2008). Brand networking capitalizes on social interactions and human relationships as a marketing tool. And actually over 60% of our respondents stated that they have joined such a group or site.

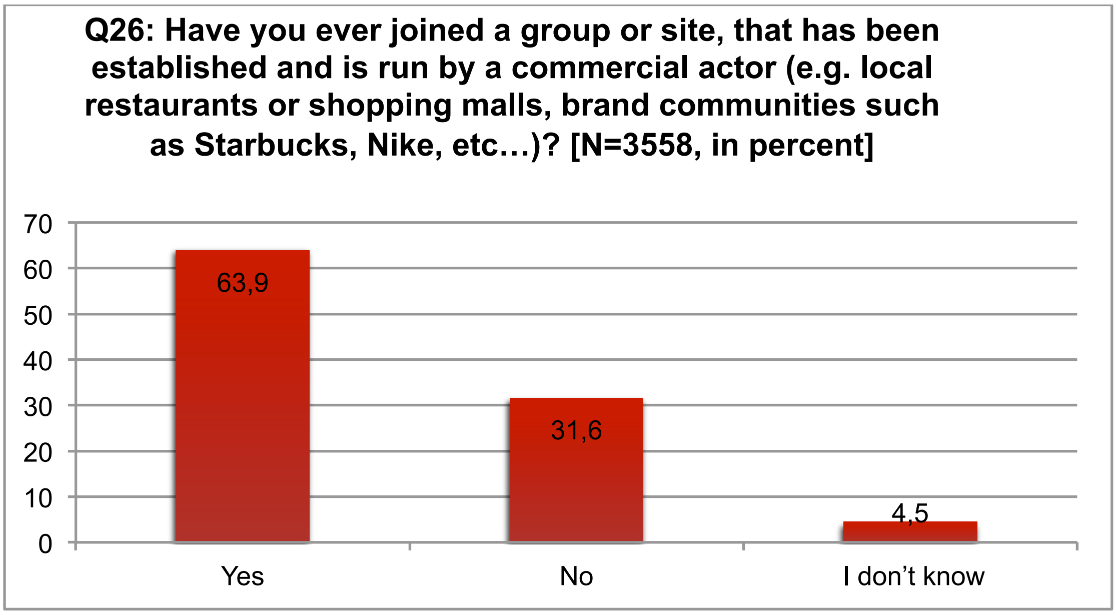


Figure 76: Results to Question 26

Comparing knowledge, attitudes and behaviour, one can observe some contradictions. Although most respondents do know that FB employs targeted advertising and clearly reject targeted advertising, they don't critically act as effect of their concern. Another example is Facebook's "social ads": If a user likes any commercial site, product or service, advertisements can be linked with his/her picture and may even be displayed in the form of a "personal recommendation among friends". Although this is a highly targeted form of advertising, nearly half of our respondents have not opted out of the social ads (the settings – of course – are by default active). Reasons may be the default setting of this option, Facebook's intransparent privacy policy, or other reasons highlighted in the interpretation section of this study.

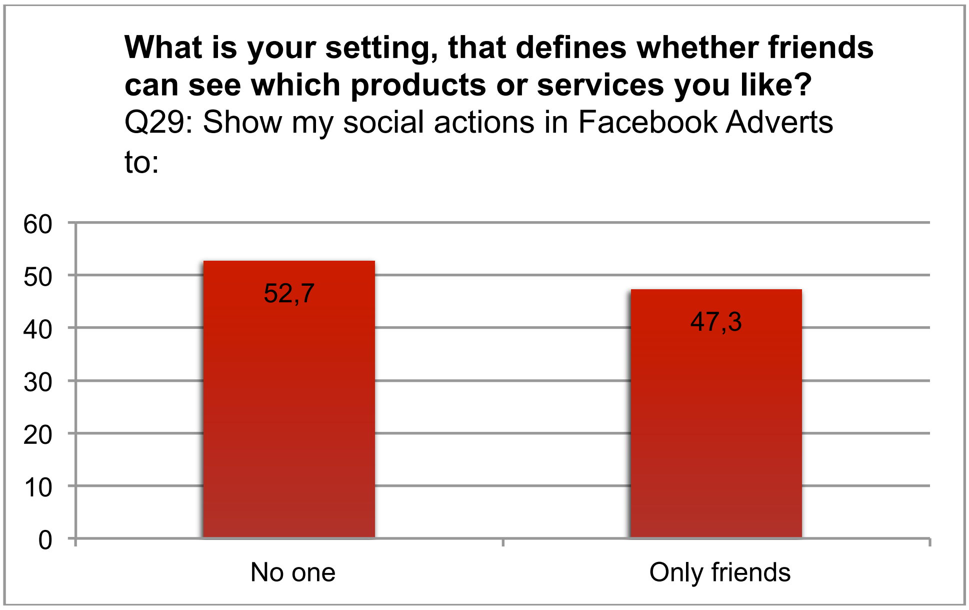


Figure 77: Results to Question 29

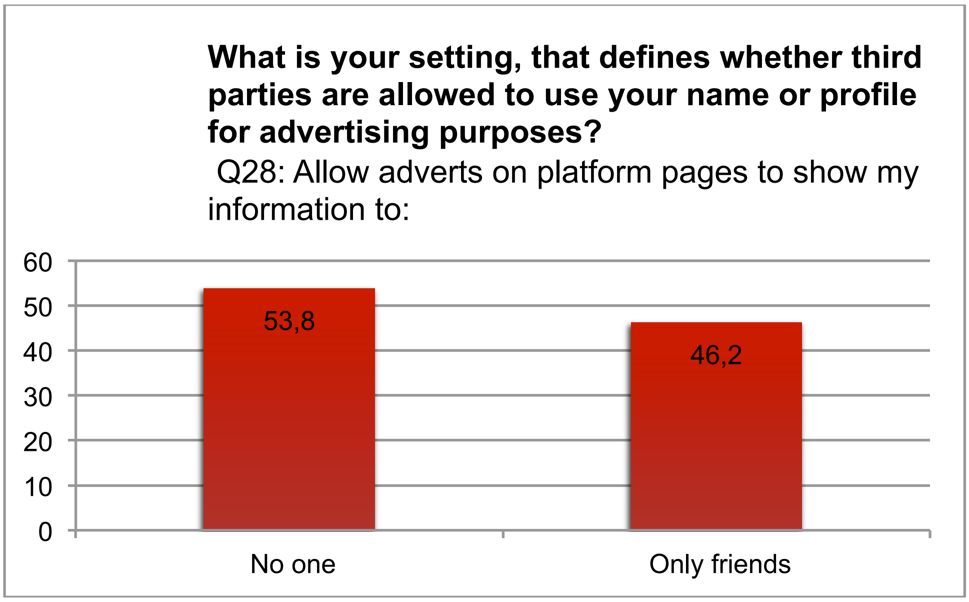


Figure 78: Results to Question 28

5. Limitations of the Study and Further Research

Although this research was carefully prepared and conducted, there are some limitations that need to be acknowledged.

First, when constructing the questionnaire we concentrated on Facebook, since it is the most popular SNS worldwide, as well as in Austria. However, in doing so, we excluded users from our study, that might use SNS except for Facebook.

Second, our study aimed to explore the usage behavior, knowledge, attitude and concerns about privacy and surveillance on SN of students. In doing so, we knowingly concentrated on a population that not only constitute a rather young age group, but also tend to be above average educated. It might be interesting to extend the scope of the study to other user groups.

Since our study reveals that a lot of respondents (83.6%) do not (or not in detail) read the privacy policy and terms of service when joining a social networking site, it might be interesting to further question users motives for not doing so. Experts have been pointing out that privacy policies are too lengthy, complicated and confusing. Further research might evaluate how a "good" (simple and clear) privacy policy should and could look like.

Our study found out that some contradictions between knowledge, attitudes and concerns and the actual behavior concerning advertising on Facebook exist. Therefore further research and in depth analysis might bring valuable insights.

Further research might explore if users who do not use Facebook or even SNS at all do so for privacy related reasons. It would be interesting if there are significant differences concerning knowledge about/attitude towards surveillance and privacy concerns between users and non-users.

6. Summary & Conclusion

In our study we explored student's usage behavior, knowledge, attitude, and concerns about surveillance and privacy on social networking sites – focusing on Facebook as the most popular SNS, and examined how these are interrelated.

First we assessed users information behavior within five categories, i.e. general usage, shared information, access, privacy settings, and advertising. We found that study respondents use Facebook quite frequently and intensely. Over three quarters (77.6%) use Facebook once or even several times a day. On average respondents write messages and update their statuses or comment on other users' statuses between several times per week and once per week; they post and share pictures on average once a month. Only a very small percentage of the respondents do not share anything at all (4.4% for status updates/comments and 12.4% for pictures). However, results imply that for a great percentage of users preserving their anonymity is important. 20.5% of our respondents use a pseudonym instead of their real name – disregarding

Facebook's name policy, which demands users to list their real, full names. Additionally, nearly a third (31.3%) declared not to be clearly identifiable on their profile picture. Only their Facebook friends are allowed to know who is behind a certain profile. However, the concept "friend" seems to be quite different on Facebook than in real life. The majority of our respondents have between 100 and 299 Facebook friends, 29.8% even have more than 300 friends on Facebook (with 2.9% having even more than 600 friends).

For better measurement of the intensity of usage we constructed an index, which shows that about half of our respondents (52.5%) fall within the category of normal users

When evaluating our respondents' information behaviour we were especially interested in how they interact with and control their profiles' privacy settings. Surprisingly, only 3% of the study participants have chosen "public" as their general privacy setting. This means that almost all of our respondents care for their privacy and have changed Facebook's default privacy setting to a more private option. The majority (57.5%) makes their profile available only to friends, and 39.5% have further customized these settings. With Facebook's constant stream of changes, keeping up with one's privacy setting can be consuming. However, a huge amount of the users try to keep up with the constant changes and adapt their settings accordingly. 65.1% of study participants have changed their settings more than three times (with 22.7% doing so more than eight times), and nearly a third (30.2%) have at least changed them once or twice.

Also, nearly three quarters of the respondents (74.6%) stated that they have blocked a Facebook Application (such as birthday calendar, FarmVille, Cities I've visited), because it accesses their data. An additional 8.2% answered that though they have never blocked an application, they are worried that some applications access a lot of their data.

These results explicitly show that users do care about their privacy on Facebook. Still, only a very low percentage of the respondents (16.4%) stated that they read the privacy policy and terms of use /service "always in detail" or at least "nearly completely". These results are quite similar to the findings from a study from the University of Queensland, which aimed at exploring the Australian communities understanding of and attitude towards online privacy (Andrejevic et al. 2012). This study found that only 18% of respondents always/most of the time read privacy policies when signing up to a website, whereas 64% rarely or never do so.

This finding further provides a basis for the claim stated by many scholars and civil rights activists that privacy policies often are lengthy, complicated and confusing (Fuchs, 2011c; Fernback and Papacharisi, 2007; Sandoval, 2010).

In order to measure how careful the study participants are in their overall information behavior on Social Networking Sites we constructed an index

(Carefulness of Information Behaviour Index). The results show that although a majority of the respondents (58.8%) show at least careful information behavior (with 28% being even very careful), still 41.2% act careless or even very careless about their informational privacy on social networking sites. Other studies such as Andrejevic et al. (2012) suggest that "younger people are more diligent with regards to providing their personal information to websites, perhaps due to being exposed to the opportunity more often due to higher levels of use". Since our sample consisted of a quite young age group (students), we might consider their more or less careful information behaviour as above average, implying that other (older) groups of society are even less careful when it comes to the amount of information shared on SNS and the chosen privacy options.

Interestingly correlation analyses between the Carefulness Index and the Intensity Index showed significantly positive results, indicating that the more intensively and actively respondents use Facebook, the more careful they are. A reason might be that heavy users have more experience in the usage of Facebook accordingly. They might be better informed about changes to privacy and advertising settings (since these are often spread via Facebook users themselves), and have invested more time in finding their way through complicated and sometimes well hidden settings. Additionally they might feel more vulnerable to privacy infringement since they upload and share a lot of data with their friends and therefore are more active in taking steps to protect their data.

Hypothesis 8*: More knowledge about surveillance is significantly positively correlated to more careful information behaviour on SNS (intensity of reading the terms of use, degree of deactivation of advertising options, degree of activation of privacy mechanisms).*

In our study we assessed how much users know about surveillance on Social Networking Sites, in digital environments as well as in general. The findings show that 75.6% of the respondents have rather low or even less surveillance knowledge, which corresponds to existing studies, suggesting that knowledge about (economic) surveillance is low (Fuchs 2009; Turow, Feldman, and Meltzer 2005; Turow, Hennessy, and Bleakley 2008; Zureik, Stalker, and Smith 2010; Phelps, Nowak, and Ferrell 2000).

In order to calculate a Surveillance- Knowledge- Index, respondents were asked if a number of eight presented statements was true or false. Also, an "I don't know"-answering category was provided.

For only three out of the eight questions a majority of the respondents knew the right answer: For Question 35 "Business organizations excessively collect and store personal information about customers" 92% answered "yes, that's true", which is the correct answer. Not quite as much, but still more than half of the respondents (62.6%) chose the right answer for Question 36 "When a Website has a privacy policy, it means that the site will not share my information with other Websites or companies". Additionally a clear majority of 83.2% was aware that the statement “On Facebook all users see the same advertisements” (Q41) is false.

Asked about the Data Retention Directive (“In Austria the Data Retention Directive by the European Union has already been implemented”) the majority of the respondents answered that they don’t know the answer (59.8%), 21.1% gave the wrong answer (Yes, that’s true), and only 19.1% knew the correct answer (No, that’s false).

For four questions the majority of the respondents checked the wrong answer.

Only 6.7% knew the correct answer to question 38 “Websites registered in Austria have to pass on personal data (e.g. name, email-address, location data, IP-address, information about whom and when you’ve sent a message or which profiles you’ve looked at] to the police upon request”. Also, asked if in Austria companies are allowed to electronically surveil their employees (e.g. monitor and analyse which websites an employee visits, which emails an employee sends or register every keystroke) (Q42), only 20.2% chose the right answer.

When asked, if it is true that Facebook is allowed to give personal data (e.g. contact information, interests, activities, friends, online behaviour) to third parties/other companies for advertising purposes, respondents were not sure about their answers. 31.8% checked “I don’t know”, another third (32.6%) thought it was correct (which is actually the right answer), and a very small majority of 35.6% answered with “ No, that’s false”.

Huge uncertainty also determined the answers to the question if advertisements, commercial sites and paid services on social networking sites, such as Facebook, must be marked as such. Only 19.4% knew the correct answer (No, that’s false), 46.5% gave the wrong answer, and 34.1% of the respondents said that they don’t know the answer.

Analysing the relationship between surveillance knowledge and the information behaviour of the participants we found them to be significantly positively correlated (validating Hypothesis 8), meaning that the more users know about surveillance the more careful they act on social networking sites.

These findings support demands for more transparency when it comes to a website’s surveillance and privacy policy, as well as public rights and laws. The low degree of surveillance knowledge within our sample suggests that there is a need for improved knowledge about surveillance practices, including data collection and targeting. It appears that more knowledge make users more alert to the omnipresent threats of surveillance and hence lead to a more careful information behaviour, in order to avert that threat. However it demonstrates that better-informed users may not be the interest of SNS providers. They might fear that more knowledge lead to a more careful information behaviour of their users, which in turn might weaken their business model of collecting, using or selling personal data.

Further examination indicates that male respondents scored higher on the Surveillance Knowledge Index. Since in contemporary society gender stereotyping still prevails, men often are more interested and educated in new technologies thereby gaining more experience and knowledge about the possibilities and threats that come along. This result corresponds to findings from Fuchs 2009 and Andrejevic et al. 2012.

Hypothesis 9: *A more critical attitude towards surveillance is significantly positively correlated to more careful information behaviour on SNS (intensity of reading the terms of use, degree of deactivation of advertising options, degree of activation of privacy mechanisms).*

Findings from our study show that students tend to have quite a critical attitude towards surveillance, with 83.8% scoring on the surveillance critique index in the categories of "very critical" or "critical". These results correspond to findings from existing studies. For example Debatin et al. (2009, 84) explored that users of social networking sites are concerned about "disclosure of personal information, damaged reputation due to rumours and gossip, unwanted contact and harassment or stalking, surveillance-like structures due to backtracking functions, use of personal data by third-parties, and hacking and identity theft". Existing studies also show that students are explicitly critical towards surveillance conducted by their current or potentials employers, whom they do not want to see personal information posted on Facebook (Christofides, Muise, and Desmarais 2009, 341; Peluchette and Karl 2008). Interestingly, in our study respondents' answers were the least critical in Q46 "It is OK, that companies screen job applicants on the Internet (e.g. on social networking sites) and search for personal information in order to reach a decision." Over 23% of the respondents agreed or totally agreed with this statement, which was the highest amount for all five statements, for which study participants were asked to indicate their agreement/disagreement. However, even here a total of about 53% was critical about such practices and disagreed or disagreed at all with the statement. In contrast, disagreement was highest (80.6% disagreed) for Q47 ("Imagine that in the course of a routine test a hospital determines that you are overweight. You think it is OK that your data is passed on to health companies, which send you offers for nutrition seminars and fitness trainings."). A possible explanation for this especially strong disagreement might be that the body (and especially weight) is considered to be the most intimate personal sphere and therefore any threat to this sphere is perceived very critically.

Analysis indicates that participants that show a more intense usage behaviour of Facebook are associated with a less critical attitude towards surveillance. Therefore we can presume that a critical attitude towards surveillance deters users to (heavily) use Facebook due to fear of surveillance.

Similarly, users that show a more critical attitude towards surveillance use Facebook in a more careful way. Hypothesis 9 has thus been validated by our findings. Also, higher surveillance knowledge correlates with a more critical attitude towards surveillance. These associations seem logical, however the findings suggest that users that are critical towards surveillance clearly perceive

SNS such as Facebook as places of surveillance and therefore adapt their information behaviour on such sites accordingly.

Hypothesis 10: *There are significant differences in information behaviour on SNS between students in the hard and the soft sciences.*

Testing for any association between the field of study of our respondents and their degree of careful information behaviour did not provide any proof for hypothesis 10, which postulates that there are significant difference in information behaviour on SNS between students in the hard and the soft sciences. Therefore our results indicate that hypothesis 10 is rejected.

We proposed this hypothesis because hard sciences rely heavily on quantifiable data and positivistic research, whereas soft sciences "also employ more qualitative methods and are more frequently confronted with critical theories and critical research in their studies than natural scientists. Positivism is only interested in how something is, whereas critical thinking is interested in suppressed potentials and in what something could become and how it can be improved. Positivism is instrumental, whereas criticism is non-instrumental" (Fuchs 2009, 64; see also Adorno 1976). Therefore we assumed that students of hard sciences tend to be less critical of social phenomena such as surveillance or threats to privacy. Assuming hypotheses 8 were proven right, (saying that a more critical attitude towards surveillance will be positively correlated with a more careful information behaviour), we argued that students of hard sciences will show a less careful information behaviour. On the contrary, studying soft sciences will increase the likelihood of being critical of surveillance, thereby increasing the likelihood of being more careful in providing information on social networking sites.

One explanation why we could not find any proof for this hypothesis, might be that the university in capitalist society no longer is a place of critical thinking at all. Soft studies have more and more become subjected to a positivist, non-critical, quantifiable-data based rationale which levelled any differences between hard and soft sciences.

Additionally, we assume that, since surveillance on social networking sites is strongly connected to data collection and electronic data processing, students of the more computer based hard sciences might be more familiar with both, surveillance technologies and the implementation of privacy protection techniques. Since hypothesis no. 7 is proven right, more knowledge increases the likelihood of more careful information behaviour. Hence, students educated in technical aspects of privacy and surveillance will show a more careful information behaviour and therefore compensate any difference in the education of critical thinking.

Hypothesis 11: *A higher degree of privacy concerns is significantly positive correlated to a more careful information behaviour on SNS (intensity of reading* *the terms of use, degree of deactivation of advertising options, degree of activation of privacy mechanisms).*

Our study aimed at exploring how much respondents are concerned about their privacy. The findings show that almost all of the participants (90.4%) are at least somewhat concerned about their privacy (47.7% concerned, 42.7% rather concerned), 8.4% rank among the "privacy pragmatists", and only 1.2% are rather unconcerned. Especially strong agreement was shown for the statement that consumers have lost all control over how personal information is collected and used by companies (88% of study participants agreed or even strongly agreed). Additionally, respondents agreed quite strongly with the presented statement that companies and Websites, such as Social Networking Sites, should never sell the personal information they have collected to other companies or Websites. Only 18.8% of the respondents felt that existing laws and organizational practices provide a reasonable level of protection for consumer privacy today. The remaining 81.2% seems to feel concerned about the level of protection granted by the state.

Findings from Andrejevic et al. (2012) even expand on that topic. They found that "almost all respondents thought all laws were necessary, covering right to privacy, do not track options, laws to protect those aged under 13 years, right to see personal information stores on websites and right to request the deletion of personal information. These findings clearly show that there is strong support for legislation to protect online privacy" (Andrejevic et al. 2012)

Further analysis showed considerable correlation between the Privacy Concern Index, the Surveillance Attitude Index and the Surveillance Knowledge Index, indicating that respondents who are more more concerned about their privacy also tended to be more critical of surveillance and/or have more knowledge about surveillance.

Validating hypothesis 11, we could find a significantly positive (but somewhat minor) correlation between the degree of privacy concern and a more careful information behaviour on SNS.

Similar results can be found in other studies: In a study about consumer's protection of online privacy and identity, Milne, Rohm and Bahl (2004) found out that "general attitudes and behaviours toward privacy were strong predictors of online privacy protection behaviour. A positive significant relationship was found for privacy concern (...) and active resistance" (Milne, Rohm, and Bahl 2004, 226). Similarly, Phelps, Nowak and Ferrell (2000) observed a strong relationship between the privacy concern level and beliefs in the importance of information protection among participants of their study about privacy concerns and consumers' willingness to provide personal information. Christofides et al. (2009, 343) argue that, although participants of their study disclosed a variety of personal and identifying information, "contrary to the assumption reports in the popular media, students in [their] survey were generally concerned about their privacy and reported that they were likely to use the variety of privacy settings" (Christofides, Muise, and Desmarais 2009, 343).

However the degree of this correlation (minor) might indicate the conflicting character of many SNS. In order to fully participate in SNS, users have to give up at least some privacy (e.g. the usage of any Facebook Application requires access to personal data) no matter how concerned they are about the related risks.

In a nutshell, our results indicate that knowledge, attitude and concerns are closely linked to the actual behaviour on social networking sites. Users who have more knowledge about surveillance and/or are more critical towards surveillance and/or are more concerned about their privacy actually show a more careful information behaviour when using social networking sites. Also more knowledge about surveillance correlates with a more critical attitude towards surveillance and a higher concern for privacy. Correlation does not necessarily imply causation. But the results of this study are indications that at the policy level more educational efforts about the commercial and surveillance risks of corporate social media are needed in order to enhance the overall rather little knowledge about these issues. Another policy recommendation is that social media platforms should be required to make their privacy policies and terms of use simpler, better understandable and that they have to provide detailed information about data collecttion and usage. Such measures require legal changes, including the possibility for sanctions and fines in the case of non-compliance. Any measures that strengthens knowledge about surveillance might lead to a more careful information behaviour as well as a more critical attitude towards surveillance and a higher concern for privacy

Focusing more closely on aspects of targeted advertising on social networking sites we found some contradictions when comparing knowledge, attitudes and behaviour.

We explored how the study respondents interact with advertisements on Facebook. About 22% admitted that they have clicked on advertisements displayed on Facebook. Asked if they have ever joined a group or site that has been established and is run by a commercial actor (e.g. local restaurants or shopping malls, brand communities such as Starbucks, Nike, etc.), a majority of 63.9% checked “yes” as an answer.

The vast majority of our respondents (82,1%) do not want websites to tailor advertisements to their personal interest. These findings are consistent with the results from other studies. Turow et al. (2008, 3) found that “even among young adults, whom advertisers often portray as caring little about information privacy, more than half (55%) of 18-24 years-old do not want tailored advertising. And contrary to consistent assertions of marketers, young adults have as strong an aversion to being followed across websites and offline (for example, in stores) as do older adults.“ Results from an Australian study show that “only one third (36%) are comfortable with tailored advertising as a concept” (Andrejevic et al. 2012, 3).

Other findings indicate that although most respondents do know that FB employs targeted advertising and clearly reject targeted advertising (82,1%), they don't critically act as effect of their concern.

Facebook provides two settings that define how someone's profile can be used for advertising purposes. Users can choose whether or not friends can see which products or services one likes and they can define whether third parties are allowed to use a user's name or profile for advertising purposes. Facebook offers two answering options "No one" and "only friends". By default the option "only friends" is activated. Only about half of our respondents have changed these settings to "no one".

When contrasting users concerns about Facebook applications with their concerns about advertising, it appears as if, because (by now) any Facebook Application has to inform its subscribers exactly about which data it accesses, users are quite careful when it comes to any application. However this caution seems to be missing when it comes to forms of data based advertising such as targeted advertising.

Despite these findings we cannot infer that the other half just does not care, but have to consider the possibility of a lack of information. These settings not only are quite hard to find, but are also relatively unknown. Additionally we should bear in mind that users hardly have any experience with such forms of advertising and the whole advertising concept is hard to grasp only by the short explanations provided by Facebook. One can conclude from these findings that though overall the study participants do care about their privacy on Facebook in general (i.e. in the form of who has access to their profiles), they seem to be less concerned about advertising practices applied on Facebook. This might be due to a lack of information and knowledge about concrete advertising methods and appropriate options to protect one's profile from these practices (choosing the right settings, blocking cookies,…). This lack of knowledge might also result in advertising not being perceived as a form of surveillance and threat to one's privacy. Additionally, advertising might be perceived as the necessary evil in order to use and connect via social networking sites such as Facebook.

Our results indicate at the policy level that it would be an advantage to implementing a legal requirement for Internet paltforms that the use of advertising is organised in the form of an opt-in. This method allows users to better agree or disagree and make informed choices

References

Acquisti, Alessandro, and Ralph Gross. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, PET 2006 Imagined Communities: Awareness, Information Sharing, and Privacy On." http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.93.8177.

Adorno, Theodor W. 1976. "Sociology and Empirical Research." In *The Positivist Dispute in German Sociology*, trans. Glyn Adey and David Frisby, 68-86. London: Heinemann.

Ajzen, Icek. 1988. *Attitudes, Personality and Behaviour*. Open University Press.

Allmer, Thomas. 2010a. *Critical Internet Surveillance Studies and Economic Surveillance*. The Internet & Surveillance-Research Paper Series. Vienna: Unified Theory of Information Research Group.

———. 2010b. *Critical Privacy Studies and the Internet*. The Internet & Surveillance-Research Paper Series. Vienna: Unified Theory of Information Research Group.

Andrejevic, Mark et al. 2012. Internet Privacy Research. Report available from http://cccs.uq.edu.au/documents/survey-results.pdf

Babbie, Earl R. 2010. *The Practice of Social Research*. Cengage Learning.

Bates, Marcia J. 2010. "Information Behavior." In *Encyclopedia of Library and Information Sciences*, ed. Marcia J. Bates and Mary Niles Maack, 3:2381-2391. 3rd ed. New York: CRC Press.

Bellman, Steven, Eric Johnson, Stephen Kobrin, and Gerald Lohse. 2004. "International Differences in Information Privacy Concerns: A Global Survey of Consumers." *The Information Society* 20 (5) (November): 313-324. doi:10.1080/01972240490507956.

Blackburn, Julia. 2003. *The Framework of Human Behaviour: 241*. Reprint. Routledge Chapman & Hall.

boyd, danah m., and Nicole B. Ellison. 2007. "Social Networking Sites: Definition, History, and Scholarship." *Journal of Computer-Mediated Communication* 13 (1).

boyd, danah m., and Eszter Hargittai. 2010. "Facebook Privacy Settings: Who Cares?" *First Monday* 15 (8).

Brewer, John, and Albert Hunter. 1989. *Multimethod Research : a Synthesis of Styles / John Brewer, Albert Hunter*. Sage Library of Social Research ; V. 175. Newbury Park, Calif. :: Sage Publications.

Buchanan, Tom, Carina Paine, Ulf-Dietrich Reips, Stefan Stieger, and Adam Joinson. 2007. "Internet Users' Perceptions of 'Privacy Concerns' and 'Privacy Actions'." *International Journal of Human-Computer Studies* 65 (6) (June): 526-536. doi:doi: DOI: 10.1016/j.ijhcs.2006.12.001.

Campbell, A J. 1997. “Relationship Marketing in Consumer Markets: A Comparison of Managerial and Consumer Attitudes About Information Privacy.” *Journal of Direct Marketing* 11 (3): 44-57. doi:10.1002/(SICI)1522-7138(199722)11:3<44::AID-DIR7>3.0.CO;2-X.

Cecez-Kecmanovic, Dubravka. 2007. . School of Information Systems, Technology and Management, Faculty of Business, UNSW, Sydney, Australia.

Chan, Yolande E., Lynda Harling Stalker, and David Lyon. 2010. *The Globalization of Personal Data Project: An International Survey on Privacy and Surveillance: Summary of Findings*. Kingston: Queen’s University.

Christofides, Emily, Amy Muise, and Serge Desmarais. 2009. “Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes?” *CyberPsychology & Behavior* 12 (3): 341-345. doi:doi: 10.1089/cpb.2008.0226.

Couper, Mick P. 2001. “Web Surveys: A Review of Issues and Approaches.” *Public Opinion Quarterly* 64 (4): 464-494.

Cronbach L. 1951. Coefficient alpha and the internal structure of tests. *Psychometrika* 16:297-333.

Davenport, Thomas H. 1997. *Information Ecology: Mastering the Information and Knowledge Environment*. 1st ed. Oxford University Press, USA.

Debatin, Bernhard, Jennette P Lovejoy, Ann-Kathrin Horn, and Brittany N Hughes. 2009. “Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences.” *Journal of Computer-Mediated Communication* 15 (1): 83-108. doi:10.1111/j.1083-6101.2009.01494.x.

Dommeyer, Curt, and Barbara Gross. 2003. “What Consumers Know and What They Do: An Investigation of Consumer Knowledge, Awareness, and Use of Privacy Protection Strategies.” *Journal of Interactive Marketing* 17 (2): 34-51. doi:10.1002/dir.10053.

Dwyer, Catherine. 2007. “Digital Relationships in the ‘MySpace’ Generation: Results from a Qualitative Study.” In *Proceedings of the 40th Hawaii International Conference on System Sciences*. Los Alamitos, CA: IEEE Press.

Evans, Joel R., and Anil Mathur. 2005. “The Value of Online Surveys.” *Internet Research* 15 (2) (January 4): 195-219. doi:10.1108/10662240510590360.

Fernback, J. & Papacharisi, Z. 2007. Online privacy as legal safeguard: The relationship among consumer, online portal, and privacy policies. *New Media & Society, 9*(5), 715-734.

Fogel, Joshua, and Elham Nehmad. 2009. “Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns.” *Computers in Human Behavior* 25 (January): 153–160. doi:10.1016/j.chb.2008.08.006.

Foucault, Michel. 1975. *Surveiller Et Punir*. Gallimard.

Frost, Pamela. 2009. “Soft Science and Hard News.” *Metanews*.

Fuchs, Christian. 2009. “Social Networking Sites and the Surveillance Society. A Critical Case Study of the Usage of StudiVZ, Facebook, and MySpace by Students in Salzburg in the Context of Electronic Surveillance.” ICT&S Center Research Report. Salzburg/Vienna.

———. 2010a. *How Can Surveillance Be Defined? Remarks on Theoretical Foundations of Surveillance Studies*. The Internet & Surveillance-Research Paper Series. Vienna: Unified Theory of Information Research Group.

———. 2010b. *Foundations of the Critique of the Political Economy of Surveillance*. The Internet & Surveillance-Research Paper Series. Vienna: Unified Theory of Information Research Group.

———. 2010c. *Critique of the Political Economy of Web 2.0 Surveillance*. The Internet & Surveillance-Research Paper Series. Vienna: Unified Theory of Information Research Group.

———. 2010d. “Social Networking Sites and Complex Technology Assessment.” *International Journal of E-Politics* 1 (3): 19-38.

———. 2011a. *The Political Economy of Privacy*. The Internet & Surveillance-Research Paper Series. Vienna: Unified Theory of Information Research Group.

———. 2011b. “Critique of the Political Economy of Web 2.0 Surveillance.” In *Internet and Surveillance: The Challenge of Web 2.0 and Social Media*, ed. Christian Fuchs, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval, in press. New York: Routledge.

———. 2011c. *Foundations of Critical Media and Information Studies*. Oxon: Routledge.

———. 2011d. “An Alternative View of Privacy on Facebook.” *Information* 2 (1) (February): 140-165. doi:10.3390/info2010140.

———. 2011e. “New Media, Web 2.0 and Surveillance.” *Sociology Compass* 5 (2) (February 1): 134-147. doi:10.1111/j.1751-9020.2010.00354.x.

———. 2011c. What is Facebook’s new privacy policy all about? More complexity, more intransparent data storage, continued Internet prosumer commodification, ideological pseudo-participation, and a reaction to the privacy complaints filed by “Europe versus Facebook”. Retrieved from http://fuchs.uti.at/699/

Gandy, Oscar. 2003. “Data Mining and Surveillance in the Post 9/11 Environment.” In *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Ag*, 26-41. London: Pluto Press.

Glaser, Barney, and Anselm Strauss. 1967. *The Discovery of Grounded Theory Glaser & Strauss 1967*. Aldine Publishing Co.

Harris Interactive. 2001a. “Privacy on & Off the Internet: What Consumers Want. Technical Report.” Harris Interactive, Inc.

———. 2001b. “Consumer Privacy Attitudes and Behaviors Survey, Conducted for the Privacy Leadership Initiative: Summary of Findings.” Harris Interactive, Inc.

Harris, Louis, and Alan F. Westin. 1990. “Consumers in the Information Age: Findings from the Survey.” Equifax.

———. 1991. “Harris-Equifax Consumer Privacy Survey 1991.” Equifax.

———. 1994. “Harris-Equifax Consumer Privacy Survey 1994: Executive Summary: Major Findings of the Survey.” Equifax. http://www.frogfire.com/frogfire_archive/equifax/consumers/privacy_survey/privacy_survey_1994.html.

———. 1995. “Harris-Equifax Consumer Privacy Survey 1995: Executive Summary: Major Findings of the Survey.” Equifax. http://www.frogfire.com/frogfire_archive/equifax/consumers/privacy_survey/privacy_survey_1995.html.

———. 1996. “Harris-Equifax Consumer Privacy Survey 1996: Executive Summary: Major Findings of the Survey.” Equifax. http://www.frogfire.com/frogfire_archive/equifax/consumers/privacy_survey/privacy_survey_1996.html.

Helmstater G. 1964. Principles of psychological measurement.. New York, Appleton-Century-Crofts.

Hiltz, S R, K. Passerini, and Catherine Dwyer. 2007. “Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace” 123.

Hinduja, Sameer, and Justin W Patchin. 2008. “Personal Information of Adolescents on the Internet: A Quantitative Content Analysis of MySpace.” *Journal of Adolescence* 31 (1) (February): 125-146. doi:10.1016/j.adolescence.2007.05.004.

Horkheimer, Max. 1972. *Critical Theory; Selected Essays*. 1st ed. Herder and Herder.

———. “Traditionelle Und Kritische Theorie.” *Zeitschrift Für Sozialforschung* 6: 245-294.

Horkheimer, Max, and Herbert Marcuse. “Philosophie Und Kritische Theorie.” *Zeitschrift Für Sozialforschung* 6: 625-647.

Howcroft, Debra, and Eileen Trauth. 2005. *Handbook of Critical Information Systems Research: Theory and Application*. Edward Elgar Publishing Ltd.

Ilieva, Janet, Steve Baron, and Nigel M Healey. 2002. “Online Surveys in Marketing Research: Pros and Cons.” *International Journal of Market Research* 44 (3): 361-376.

Kamaraguru, Ponnurangam, and Lorrie F. Cranor. 2005. "Privacy Indexes: A Survey of Westin's Studies: Research Report." http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf.

Kaplowitz, Michael D., Timothy D. Hadlock, and Ralph Levine. 2004. "A Comparison of Web and Mail Survey Response Rates." *Public Opinion Quarterly* 68 (1): 94-101.

Kehoe, J. 1995. Basic item analysis for multiple-choice tests. *Practical Assessment, Research & Evaluation, 4*(10). Retrieved August 11, 2012 from http://PAREonline.net/getvn.asp?v=4&n=10

Kellner, Douglas. "Critical Theory and the Crisis of Social Theory." (http://www.gseis.ucla.edu/faculty/kellner/kellner.html.

Kreilinger, Verena. 2010. *Remarks on Theoretical Foundations of Privacy Studies*. The Internet & Surveillance-Research Paper Series. Vienna: Unified Theory of Information Research Group.

Lefever, Samúel, Michael Dal, and Ásrún Matthíasdóttir. 2007. "Online Data Collection in Academic Research: Advantages and Limitations." *British Journal of Educational Technology* 38 (4) (July 1): 574-582. doi:10.1111/j.1467-8535.2006.00638.x.

Lewis, Kevin, Jason Kaufman, and Nicholas Christakis. 2008. "The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network." *Journal of Computer-Mediated Communication* 14 (1) (October 1): 79-100. doi:10.1111/j.1083-6101.2008.01432.x.

Lyon, David. 1994. *The Electronic Eye: The Rise of Surveillance Society*. U of Minnesota Press.

Malhotra, Naresh K., Sung S. Kim, and James Agarwal. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model." *Information Systems Research* 15 (4) (December 1): 336-355. doi:<p>10.1287/isre.1040.0032</p>.

Marcuse, Herbert. 1968. *Negations; Essays in Critical Theory*. Beacon Press.

Marx, Karl, and Friedrich Engels. 1987. *Marx Engels Collected Works*. Vol. 25. Lawrence and Wishart.

Milne, George R., and Andrew J. Rohm. 2000. "Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-In and Opt-Out Alternatives." *Journal of Public Policy & Marketing* 19 (2) (October 1): 238-249.

Milne, George R., Andrew J. Rohm, and Shalini Bahl. 2004. "Consumers' Protection of Online Privacy and Identity." *Journal of Consumer Affairs* 38 (2) (December 1): 217-232. doi:10.1111/j.1745-6606.2004.tb00865.x.

Neuman, W. Lawrence. 2006. *Basics of Social Research: Qualitative and Quantitative Approaches*. 2nd ed. Allyn & Bacon.

Nunnally J. 1978. Psychometric Theory. New York, McGraw-Hill.

Österle, Hubert, Joachim Schelp, Robert Winter, and Dubravka Cecez-Kecmanovic. 2005. "Critical Research in Information Systems: The Question of Methodology": 1446-1457.

Parrish, Margarete. 2009. *Social Work Perspectives on Human Behaviour*. Open Univ Pr.

Peluchette, Joy, and Katherine Karl. 2008. "Social Networking Profiles: An Examination of Student Attitudes Regarding Use and Appropriateness of Content." *Cyberpsychology & Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society* 11 (1) (February): 95-97. doi:10.1089/cpb.2007.9927.

Phelps, Joseph, Glen Nowak, and Elizabeth Ferrell. 2000. "Privacy Concerns and Consumer Willingness to Provide Personal Information." *Journal of Public Policy & Marketing* 19: 27-41.

Punch, Keith F. 2005. *Introduction to Social Research: Quantitative and Qualitative Approaches*. 2nd ed. Sage Publications Ltd.

Sandoval, Marisol 2011. A critical empirical case study of consumer surveillance on Web 2.0. In C. Fuchs, K. Boersma, A. Albrechtslund, & M. Sandoval (Eds.), *Internet and Surveillance: The challenge of Web 2.0 and social media*. New York: Routledge.

Sevignani, Sebastian. 2011. *A Contribution to Foundations of a Critical Theory of Privacy*. The Internet & Surveillance-Research Paper Series. Vienna: Unified Theory of Information Research Group.

Sevignani, Sebastian, Verena Kreilinger, Thomas Allmer, and Christian Fuchs. 2011. *Analysis of Existing Empirical Research Methods for Studying (Online) Privacy and Surveillance*. The Internet & Surveillance Research Paper Series. Vienna: Unified Theory of Information Research Group.

Smith, H. J., S. J. Milburg, and S. J. Burke. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices." *Mis Quarterly* 20: 167-196. doi:Article.

Statistik Austria. 2011. *Computernutzerinnen Oder Computernutzer, Internetnutzerinnen Oder Internetnutzer 2011*. IKT-Einsatz in Haushalten 2011. http://www.statistik.at/web_de/statistiken/informationsgesellschaft/ikt-einsatz_in_haushalten/index.html.

Tavani, Herman T. 1999. "Informational Privacy, Data Mining, and the Internet." *Ethics and Information Technology* 1 (2): 137-145.

———. 2008. "Informational Privacy: Concepts, Theories, and Controversies." In *The Handbook of Information and Computer Ethics*, ed. Kenneth Himma and Herman T. Tavani, 131-164. Hoboken: Wiley.

Turow, Joseph, Lauren Feldman, and Kimberly Meltzer. 2005. “Open to Exploitation: America’s Shoppers Online and Ofine.” *Annenberg School for Communication Departmental Papers*.

Turow, Joseph, Michael Hennessy, and Amy Bleakley. 2008. “Consumers’ Understanding of Privacy Rules in the Marketplace.” *Journal of Consumer Affairs* 42 (3) (September 1): 411-424. doi:10.1111/j.1745-6606.2008.00116.x.

Weber, Max. 1958. “Science as Vocation.” In *From Max Weber: Essays in Sociology*, ed. Hans H. Gerth and C. Wright Mills, 129-56. Oxford University Press (Galaxy imprint).

Wolcott, Harry F. 1992. “Posturing in Qualitative Inquiry.” In *The Handbook of Qualitative Research*, ed. M.D. LeCompte, W.L. Millroy, and J. Preissle, 3-52. San Diego: Academic Press.

Wright, Kevin B. 2005. “Researching Internet-Based Populations: Advantages and Disadvantages of Online Survey Research, Online Questionnaire Authoring Software Packages, and Web Survey Services.” *Journal of Computer-Mediated Communication* 10 (3).

Yun, Gi Woong, and Craig W Trumbo. 2000. “Comparative Response to a Survey Executed by Post, E-mail, & Web Form.” *Journal of Computer-Mediated Communication* 6 (1) (September 1): 0-0. doi:10.1111/j.1083-6101.2000.tb00112.x.

Zureik, Elia. 2004. “Overview of Public Opinion Research Regarding Privacy: Appendix A to Globalization of Personal Data Project: International Survey Concept Paper.” In . http://www.sscqueens.org/sites/default/files/Overview_Appendix_A.pdf.

Zureik, Elia, Lynda Harling Stalker, and Emily Smith. 2010. *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*. McGill-Queen’s University Press.

Appendix A: Questionnaire

In the following you can find the questionnaire used in the online survey – including the documentation of modifications (screenshots, phrasing of answer categories) due to changes in Facebook’s privacy policy and webdesign.

SURVEY QUESTIONNAIRE

Die Nutzung von Social Networking Plattformen durch Studierende an Österreichs Universitäten

Die Unified Theory of Information (UTI) Research Group führt eine Studie über das Nutzungsverhalten von Social Networking Plattformen (Facebook, Myspace, LinkedIn, etc.) durch Studenten und Studentinnen an österreichischen Universitäten durch.

Du kannst uns dabei helfen, interessante Forschungsergebnisse zu erarbeiten, indem du einen Fragebogen ausfüllst.
Dies dauert ca. 20 Minuten. Alle Daten werden vertraulich und anonym behandelt.

Es werden Amazongutscheine im Gesamtwert von 1.000 Euro (1x500€, 2x100€, 30x10€) unter jenen Teilnehmern und Teilnehmerinnen, die die Umfrage vollständig ausfüllen, verlost. Gib dazu eine E-Mail-Adresse am Ende der Umfrage an. Diese wird unabhängig von deinen Antworten verarbeitet. Es ist auch möglich, ohne Teilnahme an der Verlosung an der Umfrage teilzunehmen.

Um am Gewinnspiel teilzunehmen, musst du alle Fragen beantworten, ansonsten können wir dich beim Gewinnspiel leider nicht berücksichtigen.

Es wäre eine große Hilfe für uns, wenn du deine StudienkollegInnen, die auch Social Networking Plattformen benutzen, über diese Studie informieren könntest. Je mehr ausgefüllte Fragebögen wir erhalten, desto besser können die Forschungsergebnisse werden.

Forschungsberichte und projektrelevante Publikationen werden nach Auswertung der Daten veröffentlicht.

Kontakt:
Prof. Christian Fuchs (Projektkoordination)
UTI – Unified Theory of Information Research Group
Steinbrechergasse 15
1220 Wien
survey@uti.at
http://www.uti.at

UTI. Unified Theory of Information
Research Group

[The Usage of Social Networking Sites by Students in Austria
The Unified Theory of Information (UTI) Research Group conducts a study of Austrian students' usage behaviour of social networking platforms (studiVZ, MySpace, Facebook, etc). We appreciate if you can help is in this research by filling out a questionnaire. Completing the survey will take approximately 20 minutes. All data is treated confidentially and anonymously.

We will give away Amazon vouchers with a total value of 1.000€ (1x500€, 2x100€, 30x10€) in a lottery among the participants. Supplying your email-address is voluntary and the address will be stored independently of your survey data. It is also possible to participate in the survey without taking part in the lottery. To be considered for the lottery you need to answer all questions.
It would be of great help to us, if you inform your friends, who also use StudiVZ, about this survey. The more fully completed questionnaires we receive, the better results we will obtain. Reports on the results of the survey will be published subsequently.]

F1: Ich erkläre mich damit einverstanden, dass meine Daten für wissenschaftliche Zwecke verarbeitet und die Ergebnisse der Studie unter Einhaltung des Anonymitätsschutzes publiziert werden dürfen.
[Q1: Herewith, I agree that my personal data can be used for scientific purposes and I

have no objections that the results of the study are published in a way that does not reveal my identity.]

O Ja, ich bin damit einverstanden. [Yes, I agree.]
O Nein, ich bin damit nicht einverstanden. [No, I do not agree.]

(Verzweigungslogik: nur wenn F3: “ich nutze keine SNS”)
[Question logic: only displayed, if Q3: “I do not use any SNS”]

F2: Warum nutzt du keine Social Networking Sites? (Mehrfachnennung möglich)
[Q2: Why don’t you use any Social Networking Sites? (Multiple answers possible)]

○ Ich habe mich noch nicht damit beschäftigt.
[I haven’t looked into it.]
○ Ich pflege meine Freundschaften lieber persönlich anstelle in virtuellen Netzwerken.
[I rather cultivate my friendships personally than through virtual networks.]
○ Das ist mir zu zeitaufwändig. [It’s too time consuming.]
○ Das ist mir zu kompliziert. [It’s too complicated.]
○ Ich habe Bedenken, dass meine Privatsphäre von solchen Plattformen verletzt wird.
○ [I am concerned about my privacy being violated by such plattforms.]
○ Sonstiges (bitte angeben) [Other (please state):]

F3: Welche Social Networking Sites nutzt du? (Mehrfachnennung möglich)
[Q3: Which Social Networking Sites do you use? (Multiple answers possible)]

○ ich nutze keine Social Networking Sites [I do not use social networking sites.]
○ Facebook
○ Xing
○ LinkedIn
○ Myspace
○ studiVz
○ Andere (bitte angeben) [Other (please state):]

F4: Welche dieser Plattformen nutzt du am häufigsten?
[Q4: Which of the following platforms do you use most often?]

○ Facebook
○ Xing
○ LinkedIn
○ Myspace
○ studiVz
○ Sonstiges (bitte angeben) [Other (please state):]

F5: Wie oft führst du folgende Tätigkeiten aus?

[Q5: How often do you do the following activities?]
[Several times a day/ once a day/ several times a week/ once a week/ several times a month/ once a month/ less often/ never]

	mehrmals täglich	einmal täglich	mehrmals wöchentlich	einmal wöchentlich	mehrmals im Monat	einmal im Monat	seltener	nie
Wie oft lädst du Bilder auf Social Networking Sites, um sie mit anderen zu teilen?								
Wie oft lädst du Videos auf Social Networking Sites, um sie mit anderen zu								

	mehrmals täglich	einmal täglich	mehrmals wöchentlich	einmal wöchentlich	mehrmals im Monat	einmal im Monat	seltener	nie
teilen?								
Wie oft schreibst du Kommentare oder Statusmeldungen auf Social Networking Plattformen?								
Wie oft schreibst du Nachrichten oder chattest du mit anderen NutzerInnen auf Social Networking Sites?								

[How often do you upload pictures to social networking sites, in order to share them with others?]
[How often do you upload videos to social networking sites, in order to share them with others?]
[How often do you share a comment or status on social networking sites?]
[How often do you write messages or chat with other users on social networking sites?]

F6: Was sind für dich die größten Vorteile von Social Networking Plattformen wie Facebook, Myspace, LinkedIn, etc?

[Q6: What are the greatest advantages of social networking platforms such as Facebook, Myspace, LinkedIn, etc. for you?]

F7: Was sind deine größten Besorgnisse über Social Networking Plattformen wie Facebook, Myspace, LinkedIn, etc?

[Q7: What are your greatest concerns of social networking platforms such as Facebook, Myspace, LinkedIn, etc?]

Im folgenden Abschnitt stellen wir dir einige Fragen zu deinem Nutzungsverhalten auf Facebook.
[In the following section, we are going to ask you some questions about your usage behaviour on Facebook.]

F8: Wie oft nutzt du Facebook?
[Q8: How often do you use Facebook?]

○ mehrmals täglich [Several times a day]
○ einmal täglich [Once a day]
○ mehrmals wöchentlich [Several times a week]
○ einmal wöchentlich [Once a week]
○ mehrmals im Monat [Several times a month]
○ einmal im Monat [Once a month]
○ seltener [Less often]
○ nie [Never]

F9: Bist du auf deinem Facebook-Profilbild eindeutig zu erkennen?
[Q9: Are your clearly identifiable on your Facebook profile picture?]

○ Ja [Yes]
○ Nein [No]

F10: Verwendest du auf Facebook deinen richtigen Namen oder ein Pseudonym?
[Q10: Do you use your real name or a pseudonym on Facebook?]

○ Name [Name]
○ Pseudonym [Pseudonym]

F11: Warum verwendest du ein Pseudonym? (Mehrfachnennung möglich)
[Q11: Why do you use a pseudonym? (multiple answers possible]

- ○ weil ich Bedenken hinsichtlich des Datenschutzes habe und meinen richtigen Namen schützen möchte.
  [because I am concerned about data privacy and want to protect my real name.]
- ○ weil ich nicht will, dass mich fremde Personen finden können.
  [because I don't want people I don't know to find me.]
- ○ weil ich lieber einen kreativen/lustigen Namen wählen wollte.
  [because I preferred to choose a creative/funny name.]
- ○ Sonstiges (bitte angeben)
  [Other (please state)]

F12: Wie viele Freunde hast du auf Facebook?
[Q12: How many Facebook friends do you have?]

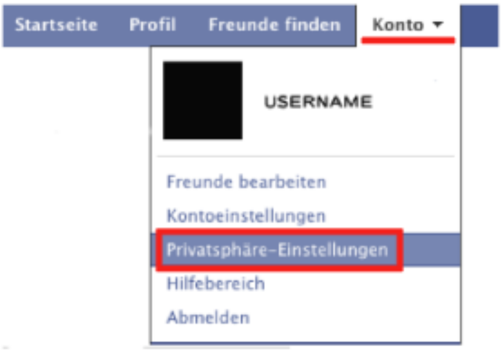
- ○ < 100
- ○ 100 - 199
- ○ 200 - 299
- ○ 300 - 399
- ○ 400 - 499
- ○ 500 - 599
- ○ > 600

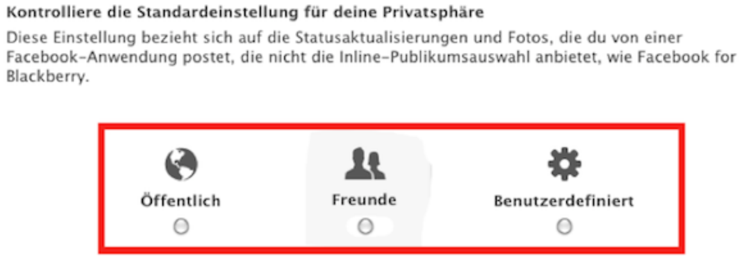
F13: Befinden sich unter deinen Facebook-Freunden auch folgende Personen:
[Q13: Among your Facebook friends are there any of the following persons:]

	Ja [Yes]	Nein [No]
ArbeitskollegInnen [Coworkers]		
Vorgesetzte an meinem Arbeitsplatz [Superiors]		
ProfessorInnen/DozentInnen [Professors/Lecturers]		

Welche Standardeinstellung für deine Privatsphäre hast du auf Facebook gewählt?
[Which privacy settings have you chosen for Facebook?]

Solltest du dir nicht sicher sein, mit wem du auf Facebook deine Informationen teilst, bitten wir dich, dich auf Facebook einzuloggen und uns, ohne Änderungen zu machen, mitzuteilen, was du dort angibst. Du findest diese Einstellung rechts oben unter „Konto" – „Privatsphäre-Einstellungen".
[If you were not sure with whom you are sharing your data on Facebook, we would ask you to log in to your Facebook profile and - without making any changes – to tell us your privacy settings.]





Kontrolliere die Standardeinstellung für deine Privatsphäre

Diese Einstellung bezieht sich auf die Statusaktualisierungen und Fotos, die du von einer Facebook-Anwendung postest, die nicht die Inline-Publikumsauswahl anbietet, wie Facebook for Blackberry.

Öffentlich ○ Freunde ○ Benutzerdefiniert ○

F14: Bitte wähle die zutreffende Antwort aus:
[Q14: Please choose the appropriate answer:]

- ○ Öffentlich [Public]
- ○ Freunde [Friends]
- ○ Benutzerdefiniert [Custom]

F16: Wenn du dich bei einer Social Networking Plattform anmeldest oder diese nutzt, liest du deren Nutzungs- und Datenschutzbestimmungen?
[Q16: When you join or use a social networking site, do you read the privacy policy and terms of service?]

- ○ Nein, nie [No, never]
- ○ Oberflächlich oder fast gar nicht [Superficially/Hardly ever]
- ○ Teilweise [Partially]
- ○ Fast vollständig [Nearly completely]
- ○ Immer im Detail [Always in detail]

(Verzweigungslogik: nur angezeigt, wenn bei S12_F16 „teilweise“, „fast vollständig“ oder „immer im detail“)
[Question logic: only displayed, if Q16: partially/nearly completely/always in detail]

F17: Beeinflusst diese Information in irgendeiner Weise dein Verhalten auf solchen Plattformen?
[Q17: Does this information influence your behaviour on such sites in any way?]

- ○ Ja, ich habe mehr Vertrauen und teile mehr persönliche Daten
  [Yes, I have more trust and share my personal information]
- ○ Ja, ich bin vorsichtiger und teile weniger persönliche Daten
  [Yes, I am more cautious and share less personal information]
- ○ Nein [No]
- ○ Ich weiß nicht [I don’t know]

F18: Hast du an den voreingestellten Privatsphäre-Einstellungen auf Facebook schon einmal etwas geändert? Wenn ja, wie oft?
[Q18: Have you ever changed the default privacy settings for Facebook? If yes, how often?]

- ○ Nein, noch nie [No, never.]

- ○ Ja, ein- oder zweimal [Yes, once or twice.]
- ○ Ja, drei- bis achtmal [Yes, three to eight times.]
- ○ Ja, häufiger als achtmal [Yes, more often than eight times.]
- ○ Ich weiß nicht [I don’t know.]

F19: Hast du schon einmal eine Facebook-Anwendung (wie z.B. Geburtstagskalender, FarmVille, Cities I’ve visited, ...) blockiert, weil sie auf deine Daten zugreift?
[Q19: Have you ever blocked a Facebook Application (as e.g. birthday calendar, FarmVille, Citiies I’ve visited,…),because it accesses your data?]

- ○ Ja [Yes]
- ○ Nein, das stört mich nicht [No, that doesn’t bother me.]
- ○ Nein, aber es beunruhigt mich, wenn ich sehe, dass Anwendungen auf viele meiner Daten zurückgreifen
  [No, but it worries me, when I see, that some applications access a lot of my data.]
- ○ Ich habe noch nie eine Facebook-Anwendung aufgerufen oder verwendet.
  [I have never activated or used a Facebook Application.]
- ○ Ich weiß nicht [I don’t know.]

F20: Wenn Facebook Änderungen in den Datenschutz- oder Nutzungsrichtlinien durchführt ohne die NutzerInnen darüber zu informieren, wird diese Information häufig von anderen NutzerInnen mittels Status-Updates verbreitet. Wie denkst du über diese informelle Form der Verbreitung? (Mehrfachnennung möglich)

[Q20: When Facebook changes its privacy policy or terms of service without user notification, regularly some users spread these changes via their status updates. How do you feel about this informal way of information dissemination? (Multiple answers possible)]

- ○ Ich finde das störend. Wenn es sich um eine wirklich wichtige und für mich relevante Änderung handelt, wird Facebook mich darüber informieren.
  [I find it annoying. If it really is an important and relevant matter, Facebook will inform me.]
- ○ Ich finde das hilfreich, weil ich dadurch besser informiert bin.
  [I find it helpful, because thus I’m better informed.]
- ○ Ich finde es wichtig, dass die NutzerInnen aufmerksam sind und Facebook Änderungen nicht so leicht durchführen kann, ohne dass ich davon erfahre.
  [I find it important that users are attentive and make it harder for Facebook to make any modifications without notifying me.]
- ○ Darüber habe ich noch nie nachgedacht/ mir ist das noch nie aufgefallen.
  [I have never thought about that/I have never noticed that.]
- ○ Sonstiges (bitte angeben) [Other (please state)]

(Verzweigungslogik: nur angezeigt, wenn bei S14_F20 antwortmöglichkeit 2,3 oder 5 ausgewählt wurde)
[Question logic: only displayed, if Q20 answer 2,3 or 5]

F21: Hast du selbst schon einmal andere NutzerInnen über Änderungen der Datenschutzbedingungen- und/oder Nutzungsbedingungen informiert?
[Q21: Have you yourself ever participated in informing other users about changes in the privacy policy or terms of service?]

- ○ Ja [Yes]
- ○ Nein [No]

F22: Wie oft liest du die Werbeanzeigen, welche auf deinem Facebook-Profil auf der rechten Seite eingeblendet warden?

[Q22: How often do you read the advertisements, which are displayed on the right side of your Facebook Profile?]

- ○ mehrmals täglich [Several times a day]
- ○ einmal täglich [Once a day]
- ○ mehrmals wöchentlich [Several times a week]
- ○ einmal wöchentlich [Once a week]
- ○ mehrmals im Monat [Several times a month]
- ○ einmal im Monat [Once a month]
- ○ seltener [Less often]
- ○ nie [Never]

F23: Hast du schon einmal auf eine Werbeanzeige auf Facebook geklickt?
[Q22: Have you ever clicked on an advertisement displayed on Facebook?]

- ○ Ja [Yes]
- ○ Nein [No]
- ○ Ich weiß nicht [I don't know]

(Verzweigungslogik: nur angezeigt, wenn bei S16_F23 „ja")
[Question logic: only displayed, if Q23 "yes"]

F24: Wie oft klickst du auf Werbeanzeigen auf Facebook?
[Q24: How often do you click on advertisements on Facebook?]

- ○ mehrmals täglich [Several times a day]
- ○ einmal täglich [Once a day]
- ○ mehrmals wöchentlich [Several times a week]
- ○ einmal wöchentlich [Once a week]
- ○ mehrmals im Monat [Several times a month]
- ○ einmal im Monat [Once a month]
- ○ seltener [Less often]
- ○ nie [Never]

F25: Wann klickst du auf Werbeanzeigen? (Mehrfachnennung möglich)
[Q25: In which case do you click on advertisements? (multiple answers possible)]

- ○ wenn es sich um ein für mich relevantes Produkt/Service handelt.
  [if the product/service is relevant to me.]
- ○ wenn ich mehr über das Produkt/den Service herausfinden will.
  [if I want to learn more about the product/service.]
- ○ wenn die Anzeige ansprechend gestaltet ist.
  [if the advertisement is appealing in its design.]
- ○ wenn es sich um ein gutes Angebot handelt.
  [if it is a good offer.]
- ○ Sonstiges (bitte angeben)
  [Other (please state)]

F26: Bist du auf Facebook schon einmal einer Gruppe oder Seite beigetreten, welche von einem kommerziellen Anbieter erstellt & betrieben wird (zb. Seiten lokaler Gastronomiebetriebe oder Einkaufszentren, Communities großer Marken wie Starbucks, Nike, usw.)?
[Q26: Have you ever joined a group or site, that has been established and is run by a commercial actor (e.g. local restaurants or shopping malls, brand communities such as Starbucks, Nike, etc…)?]

- ○ Ja (Yes)
- ○ Nein (No)
- ○ Ich weiß nicht (I don't know)

(Verzweigungslogik: nur angezeigt, wenn bei S18_F26 „ja“)
[Question logic: only displayed, if Q26 “yes”}

F27: Was sind Gründe dafür, dass du solchen Seiten oder Gruppen beitrittst? (Mehrfachnennung möglich)
[What are your reasons for joining such a site or group? (multiple answers possibles]

○ um Informationen über Neuheiten, Spezialangebote, etc. zu erhalten.
[to receive information about news, special offers etc..]

○ weil ich mich mit der Marke/dem Anbieter identifizieren kann.
[because I can identify with the brand/provider.]

○ um meine Freunde darauf aufmerksam zu machen.
[in order to draw my friends’ attention to it.]

○ weil mir die Seite/Gruppe gut gefallen hat.
[because I like the site or group.]

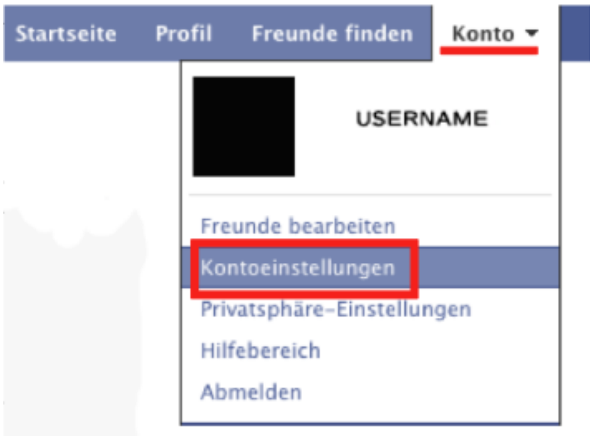
○ weil es ein Gewinnspiel oder ein spezielles Angebot für Mitglieder gibt.
[because there is a lottery or special offering for members.]

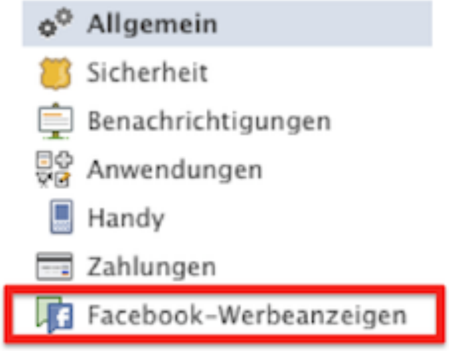
○ um andere Menschen kennenzulernen, welche sich für dieselben Produkte/Services interessieren.
[in order to get to know other people that are interested in the same product/service.]

○ Sonstiges (bitte angeben)
[Other (please state)]

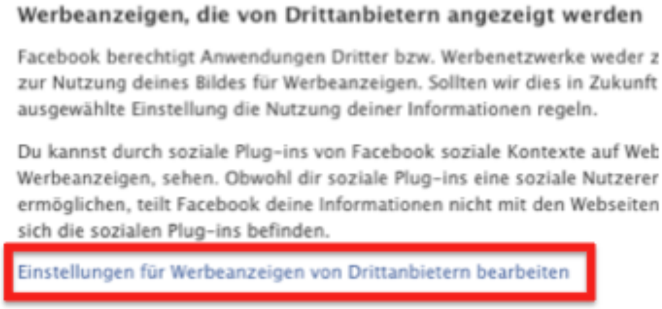
Wir bitten dich nun, dich bei Facebook einzuloggen, deine Werbeeinstellungen anzusehen und uns dann, ohne Änderungen zu machen, ehrlich zu sagen, wie deine Einstellungen aussehen. Du findest diese Einstellungen unter "Konto – Kontoeinstellungen – Facebook-Werbeanzeigen".

[We will now ask you to login to your Facebook profile, look at your advertising settings and to – without making any changes – honestly tell us, which preferences are set. You can find these settings under “Account” – “Account Settings” – “Facebook Advertsiements”.]





Was zeigt deine Einstellung, welche bestimmt, ob dein Name oder Profilbild von Drittanbietern für Werbezwecke verwendet werden darf?
[What is your setting, that defines whether third parties are allowed to use your name or profile for advertising purposes?]

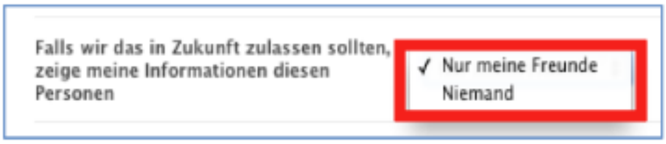


Werbeanzeigen, die von Drittanbietern angezeigt werden

Facebook berechtigt Anwendungen Dritter bzw. Werbenetzwerke weder z
zur Nutzung deines Bildes für Werbeanzeigen. Sollten wir dies in Zukunft
ausgewählte Einstellung die Nutzung deiner Informationen regeln.

Du kannst durch soziale Plug-ins von Facebook soziale Kontexte auf Wet
Werbeanzeigen, sehen. Obwohl dir soziale Plug-ins eine soziale Nutzerer
ermöglichen, teilt Facebook deine Informationen nicht mit den Webseiten
sich die sozialen Plug-ins befinden.

Einstellungen für Werbeanzeigen von Drittanbietern bearbeiten



Falls wir das in Zukunft zulassen sollten, zeige meine Informationen diesen Personen

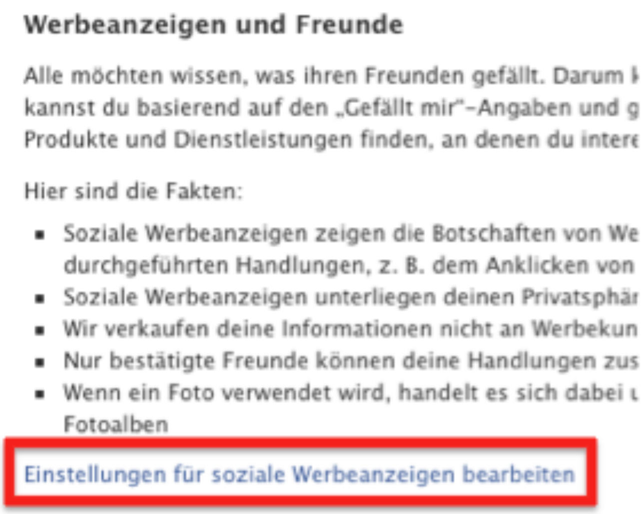
✓ Nur meine Freunde
Niemand

F28: Falls wir das in Zukunft zulassen sollten, zeige meine Informationen diesen Personen:

[Q28: Allow adverts on platform pages to show my information to:]

- ○ Niemand (No one)
- ○ Nur meine Freunde (Only friends)

Was zeigt deine Einstellung, welche bestimmt, ob deinen Freunden angezeigt wird, welche Produkte oder Services dir gefallen?
[What is your setting, that defines whether friends can see which products or services you like?]



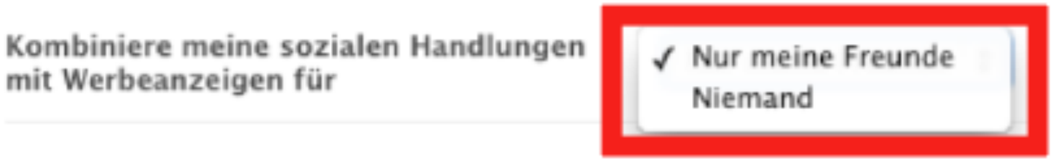
Werbeanzeigen und Freunde

Alle möchten wissen, was ihren Freunden gefällt. Darum k
kannst du basierend auf den „Gefällt mir"-Angaben und g
Produkte und Dienstleistungen finden, an denen du intere

Hier sind die Fakten:

- Soziale Werbeanzeigen zeigen die Botschaften von We
  durchgeführten Handlungen, z. B. dem Anklicken von
- Soziale Werbeanzeigen unterliegen deinen Privatsphär
- Wir verkaufen deine Informationen nicht an Werbekun
- Nur bestätigte Freunde können deine Handlungen zus
- Wenn ein Foto verwendet wird, handelt es sich dabei u
  Fotoalben

Einstellungen für soziale Werbeanzeigen bearbeiten



Kombiniere meine sozialen Handlungen mit Werbeanzeigen für

✓ Nur meine Freunde
Niemand

F29: Kombiniere meine soziale Handlungen mit Werbeanzeigen für:
[Q29: Show my social actions in Facebook Adverts to]

- ○ Niemand (No one)
- ○ Nur meine Freunde (Only friends)

F30: Wurde dir online schon einmal eine Werbeanzeige gezeigt, welche auf deinen Interessen und/oder deinem Surfverhalten basierte?

[Q30: Have you ever been shown an advertisement, which was based on your interests and/or online behaviour?]

- ○ Ja [Yes]
- ○ Nein [No]
- ○ Ich weiß nicht [I don't know]

F31: Möchtest du, dass Webseiten, die du besuchst, dir Werbeanzeigen zeigen, welche auf deine persönlichen Interessen zugeschnitten sind?

[Q31: Do you want websites that you visit to tailor advertisements to your personal interest?]

- ○ Ja, möchte ich (Yes, I'd like that.)
- ○ Nein, möchte ich nicht (No, I wouldn't like that.)

(*Verzweigungslogik: nur angezeigt, wenn bei S21_F31 „ja"*)
(Question logic: only displayed, if Q31 "yes")

F32: Ist es für dich in Ordnung, wenn diese Werbeanzeigen auf dich abgestimmt werden, indem die folgenden Aktivitäten von Werbekunden einer Webseite gespeichert und analysiert werden:
[Q32: Would it be OK if these ads were tailored for you based on the storage and analysis of the following activities by advertisers of a website:]
[yes/no/I don't know]

ja nein weiß nicht

	ja	nein	weiß nicht
Dein Verhalten auf der Webseite, auf der die Werbung angezeigt wird (was du dir ansiehst, worauf du klickst, welche Profile du ansiehst,...) [What you do on the website that displays the advertisement (what you look at, what you click on, which profiles you visit…)]			
Dein generelles Online-Verhalten (welche Webseiten du dir im gesamten WWW ansiehst, welche Suchanfragen du zB. bei Google eingibst, wie lange du dir eine Webseite ansiehst, usw.) [your online behaviour in general (which websites you visit on the whole www, which search requests you make e.g. on Google, how long you visit a certain website, etc.]			
Dein Facebook-Profil (z.B. welche Interessen du dort angibst, welche Gruppen du beitrittst, welche Aktivitäten und Links du dort postest) [your Facebook Profile (e.g. your interests, groups, you've joined, activities & links, you've posted)]			
Deine Facebook-Kontakt/Freundesliste [your Facebook contacts/friends-list]			
Deine E-Mails (z.B. an wen du Nachrichten per Facebook oder Google-Mail schickst, der Inhalt dieser E-Mails) [your emails (e.g. whom you send message via Facebook or GoogleMail, the content of these mails,…)]			
Deinen Aufenthaltsort (z.B. standortbezogene Daten durch Mobiles Internet, Fotos, die du hochlädst, oder die Facebook-Anwendung "Orte, die du besuchst/Places") [your location (e.g. location based data via mobile internet, pictures, you've uploaded, or the Facebook-Application "Places")]			

F33: Ist es für dich in Ordnung, wenn basierend auf deinen Facebook-Profildaten...
[Q33: Would it be OK if based on your Facebook Profile….]
[Yes/No/Idon't know]

	ja	nein	weiß nicht
Werbeanzeigen auf Facebook auf deine persönlichen Interessen zugeschnitten werden - ohne dass Facebook diese Daten an externe Werbeunternehmen weitergibt [ads on Facebook were tailored to your personal interest – without Facebook giving the data away to external advertisers.]			
Werbeanzeigen auf anderen Webseiten auf deine persönlichen Interessen zugeschnitten werden - indem Facebook diese Daten an externe Werbeunternehmen weitergibt [ads on Facebook were tailored to your personal interest – by Facebook giving the data away to external advertisers.]			

F34: Wie würdest du dein Wissen über Datenschutzgesetze, Privatsphäre-Richtlinien, sowie Überwachungs-Methoden und -Maßnahmen von staatlichen Akteuren (z.b. Polizei) sowie Unternehmen (speziell auch Betreibern von Social Networking Sites) einschätzen?

[Q34: How knowledgeable do you feel about data protection acts, privacy guidelines, as well as surveillance methods and practices used by governmental actors (e.g. police) as well as private companies (especially providers of social networking sites)?]

- ○ Sehr hoch [Extremely knowledgeable]
- ○ Hoch [Very knowledgeable]
- ○ Mittel [Somewhat knowledgeable]
- ○ Gering [Less knowledgeable]
- ○ Sehr gering [Not at all knowledgeable]

Welche Antworten zu den folgenden Fragen sind richtig? Bitte antworte spontan entsprechend deinem Wissensstand. Wenn du dir nicht sicher bist, kreuze einfach „ich weiß nicht" an.
[What are the correct answers to the following questions? Please answer spontaneously without looking it up. If you are not sure, just check "I don't know"]

F35: Unternehmen und Konzerne sammeln und speichern in großem Ausmaß persönliche Informationen über ihre KundInnen.
[Q35: Business organizations excessively collect and store personal information about customers]

- ○ Ja, das stimmt [Yes, that's true.]
- ○ Nein, das stimmt nicht [No, that's false.]
- ○ Ich weiß nicht [I don't know.]

F36: Wenn eine Webseite eine Datenschutzerklärung hat, bedeutet das, dass sie meine persönlichen Daten nicht an andere Webseiten oder Unternehmen weitergibt.
[Q36: When a Website has a privacy policy, it means that the site will not share my information with other Websites or companies]

- ○ Ja, das stimmt [Yes, that's true.]
- ○ Nein, das stimmt nicht [No, that's false.]
- ○ Ich weiß nicht [I don't know.]

F37: In Österreich wurde die von der EU eingeforderte Vorratsdatenspeicherung bereits eingeführt.
[Q37: In Austria the Data Retention Directive by the European Union has already been implemented]

- ○ Ja, das stimmt [Yes, that's true.]
- ○ Nein, das stimmt nicht [No, that's false.]
- ○ Ich weiß nicht [I don't know.]

F38: In Österreich registrierte Webseiten müssen gewisse persönliche Daten (z.B. Name, E-Mail-Adresse, Standortdaten, IP-Adresse, Information darüber, wem du wann eine Nachricht gesendet hast oder welche Profile du dir angesehen hast) an die österreichische Polizei weitergeben, wenn diese das verlangt.
[Q38: Websites registered in Austria have to pass on personal data (e.g. name, email-address, location data, IP-address, information about whom and when you've sent a message or which profiles you've looked at] to the police upon request.]

- ○ Ja, immer dann, wenn die Polizei das verlangt.
  [Yes, always if the police demand it.]
- ○ Nein, niemals. [No, never.]
- ○ Nur dann, wenn die Polizei eine richterliche Genehmigung angefordert hat, diese vom Richter genehmigt wird und an die Plattform ausgehändigt wird.
  [Only if the police have a juridical order that was passed by a court and is handed over to the provider.]
- ○ Ich weiß nicht. [I don't know.]

F39: Facebook darf meine persönlichen Daten (z.B. Kontaktinformation, Interessen, Aktivitäten, Freunde, Surfverhalten) an andere Unternehmen für Werbezwecke weitergeben.
[Q39: Facebook is allowed to give my personal data (e.g. contact information, interests, activities, friends, online behaviour) to third parties/other companies for advertising purposes.]

- ○ Ja, das stimmt [Yes, that's true.]
- ○ Nein, das stimmt nicht [No, that's false.]
- ○ Ich weiß nicht [I don't know.]

F40: Werbung, kommerzielle Seiten und bezahlte Dienstleistungen müssen auf Social Networking Sites wie Facebook als solche auch gekennzeichnet werden.
[Q40: Advertisements, commercial sites and paid services on social networking sites, such as Facebook, must be marked as such.]

- ○ Ja, das stimmt [Yes, that's true.]
- ○ Nein, das stimmt nicht [No, that's false.]
- ○ Ich weiß nicht [I don't know.]

F41: Alle User sehen auf Facebook dieselben Werbeanzeigen.
[Q41: On Facebook all users see the same advertisements.]

- ○ Ja, das stimmt [Yes, that's true.]
- ○ Nein, das stimmt nicht [No, that's false.]
- ○ Ich weiß nicht [I don't know.]

F42: In Österreich dürfen Unternehmen ihre Mitarbeiter elektronisch überwachen (z.B. auswerten welche Internet-Seiten eine Mitarbeiterin abruft, welche E-Mails ein Mitarbeiter schreibt oder auch das Registrieren jeden Tastendrucks).
[Q42: In Austria companies are allowed to electronically surveil their employees (e.g. monitor and analyse which websites an employee visits, which emails an employee sends or register every keystroke)]

- ○ Ja, das stimmt. Unternehmen dürfen ihre MitarbeiterInnen überwachen.
  [Yes that's true. Companies are allowed to monitor their employees.]
- ○ Nein, das stimmt nicht. Überwachung am Arbeitsplatz ist in Österreich in jedem Fall gesetzlich verboten.
  [No, that's false. In any case, workplace surveillance is prohibited in Austria.]
- ○ Ich weiß nicht (I don't know.)

Was denkst du über folgende Aussagen:
[How do you feel about the following statements:]
[totally agree/agree/neutral/don't agree/don't agree at all]

F43: Wer nichts Illegales zu verbergen hat, braucht vor Überwachung keine Angst zu haben.
[Q43: If you have nothing illegal to hide, then you need not be afraid of surveillance.]

	stimme völlig zu	stimme zu	bin neutral (teils/teils)	stimme nicht zu	stimme gar nicht zu
Ich...	○	○	○	○	○

F44: Wir brauchen mehr Überwachung um uns vor steigender Kriminalität, Sexualstraftätern und Terroristen schützen und in Sicherheit leben zu können.
[Q44: We need more surveillance in order to protect ourselves from increasing crime, sex predators, and terrorists so as to be able to live in safety.]

	stimme völlig zu	stimme zu	bin neutral (teils/teils)	stimme nicht zu	stimme gar nicht zu
Ich...	○	○	○	○	○

F45: Wenn Unternehmen persönliche Dinge über mich wissen, schadet mir das nicht.
[Q45: It won't hurt me if companies know personal information about me.]

	stimme völlig zu	stimme zu	bin neutral (teils/teils)	stimme nicht zu	stimme gar nicht zu

	stimme völlig zu	stimme zu	bin neutral (teils/teils)	stimme nicht zu	stimme gar nicht zu
Ich...	○	○	○	○	○

F46: Ich finde es in Ordnung, dass Unternehmen Job-BewerberInnen im Internet (zum Beispiel auf Social Networking Seiten) durchleuchten und nach persönlichen Informationen suchen, um ihre Entscheidung zu treffen.
[Q46: It is OK, that companies screen job applicants on the Internet (e.g. on social networking sites) and search for personal information in order to reach a decision.]

	stimme völlig zu	stimme zu	bin neutral (teils/teils)	stimme nicht zu	stimme gar nicht zu
Ich...	○	○	○	○	○

F47: Stell dir vor, dass im Krankenhaus bei einer Routineuntersuchung festgestellt wird, dass du übergewichtig seist. Du findest es in Ordnung, dass deine Daten an Unternehmen der Gesundheitsbranche weitergeben werden und du Angebote zu Ernährungsseminaren und Fitnesskursen erhältst.

[Q47: Imagine that in the course of a routine test a hospital determines that you are overweight. You think it is OK that your data is passed on to health companies, which send you offers for nutrition seminars and fitness trainings.]

	stimme völlig zu	stimme zu	bin neutral (teils/teils)	stimme nicht zu	stimme gar nicht zu
Ich...	○	○	○	○	○

F48: Was würdest du darüber denken, wenn die unten genannten Organisationen persönliche Informationen über dich an andere Unternehmen weitergeben würden?
[Q48: How would you feel about the following organisations giving away personal information to other companies?]
[Totally alright/ Alright/ Neutral/ Not alright/ Not at all alright]

	ich finde das völlig in Ordnung	ich finde das in Ordnung	mir ist das egal	ich finde das nicht in Ordnung	ich finde das gar nicht in Ordnung
Dein Internet Service Provider gibt Daten über dein Surfverhalten an andere Unternehmen weiter. [Your Internet Service Provider gives away data on your online behaviour.]	○	○	○	○	○
Dein Kreditkartenunternehmen gibt Daten über dein Einkaufsverhalten an andere Unternehmen weiter. [Your credit card company gives away data on your buying behaviour.]	○	○	○	○	○
Ein Onlineshop wie Amazon gibt Daten über deine Onlineeinkäufe an andere Unternehmen weiter. [an online shop such as Amazon gives away data on your purchase.]	○	○	○	○	○
Social Networking Sites wie z.B. Facebook geben Daten über deine Interessen an andere Unternehmen weiter. [Social Networking Sites such as Facebook give away data on your	○	○	○	○	○

	ich finde das völlig in Ordnung	ich finde das in Ordnung	mir ist das egal	ich finde das nicht in Ordnung	ich finde das gar nicht in Ordnung
personal interests]					
Social Networking Sites wie z.B. Facebook geben Daten über die von dir besuchten Profile und Gruppen an andere Unternehmen weiter. [Social Networking Sites such as Facebook give away information about the profiles and groups you've visited]	○	○	○	○	○

Wir zeigen dir nun einige Aussagen. Bitte teile uns mit, inwiefern du diesen zustimmst.
[We will now show you some statements. Please tell us whether or not you agree with them.]
[I…Strongly agree/ Agree/ Disagree/ Strongly disagree]

F49: KonsumentInnen haben jegliche Kontrolle darüber verloren, wie persönliche Daten über sie von Unternehmen gesammelt und verwendet werden.
[Q49: Consumers have lost all control over how personal information is collected and used by companies.]

	stimme völlig zu	stimme zu	stimme nicht zu	stimme gar nicht zu
Ich...	○	○	○	○

F50: Die meisten Unternehmen handhaben persönliche Daten, welche sie von KonsumentInnen gesammelt haben, in angemessener und vertraulicher Art und Weise.
[Q50: Most businesses handle the personal information they collect about consumers in a proper and confidential way.]

	stimme völlig zu	stimme zu	stimme nicht zu	stimme gar nicht zu
Ich...	○	○	○	○

F51: Bestehende Gesetze und Unternehmenspraktiken bieten gegenwärtig ein ausreichendes Maß an Schutz der Privatsphäre von KonsumentInnen.
[Q51: Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.]

	stimme völlig zu	stimme zu	stimme nicht zu	stimme gar nicht zu
Ich...	○	○	○	○

Wir zeigen dir nun einige Aussagen. Bitte teile uns mit, inwiefern du diesen zustimmst.
[We will now show you some statements. Please tell us whether or not you agree with them.]
[I…Strongly agree/ agree/ Slightly agree/ Neither agree nor disagree/ Slightly disagree/ Disagree/ Strongly disagree]

F52: Wenn Webseiten mich um persönliche Daten fragen, überlege ich manchmal zweimal bevor ich diese angebe.
[Q52: When Websites ask me for personal information, I sometimes think twice before providing it.]

	stimme völlig zu	stimme zu	stimme eher zu	teils/teils	stimme weniger zu	stimme nicht zu	stimme gar nicht zu

	stimme völlig zu	stimme zu	stimme eher zu	teils/teils	stimme weniger zu	stimme nicht zu	stimme gar nicht zu
Ich...	○	○	○	○	○	○	○

F53: Unternehmen und Webseiten, wie z.B. Social Networking Sites, sollen mehr Zeit und Kosten aufwenden um persönliche Daten vor unautorisiertem Zugriff zu schützen.
[Q53: Companies and Websites, such as Social Networking Sites, should devote more time and effort for preventing illegal access to personal information.]

	stimme völlig zu	stimme zu	stimme eher zu	teils/teils	stimme weniger zu	stimme nicht zu	stimme gar nicht zu
Ich...	○	○	○	○	○	○	○

F54: Online-Unternehmen sollen sicherstellen, dass persönliche Daten, welche sie über ihre KundInnen sammeln und speichern, korrekt und fehlerfrei sind – egal wie viel das kostet.
[Q54: Internet companies should make sure that all personal information they have collected and stored about their customers, is true and accurate – no matter how much this costs.]

	stimme völlig zu	stimme zu	stimme eher zu	teils/teils	stimme weniger zu	stimme nicht zu	stimme gar nicht zu
Ich...	○	○	○	○	○	○	○

F55: Unternehmen und Webseiten, wie z.B. Social Networking Sites, sollen niemals persönliche Daten, welche sie gesammelt haben, an andere Unternehmen oder Websites weiterverkaufen.
[Q55: Companies and Websites, such as Social Networking Sites, should never sell the personal information they have collected to other companies or Websites.]

	stimme völlig zu	stimme zu	stimme eher zu	teils/teils	stimme weniger zu	stimme nicht zu	stimme gar nicht zu
Ich...	○	○	○	○	○	○	○

Teile uns bitte im Folgenden deinen wichtigsten Grund mit, der dafür bzw. dagegen spricht:
[Please tell us your most important reason for or against the following questions.]

F56: Sollte deine Handynummer auf Facebook für alle Menschen sichtbar sein oder nicht? Was ist der wichtigste Grund, der dafür bzw. dagegen spricht?
[Q56: Should your mobile phone number be visible to all people on Facebook, or not? What is the most important reason for or against it?]

- ○ Ja, Facebook ist wie ein Telefonbuch. Ich bin froh, wenn Menschen, die mich suchen auch finden können, um mich zu kontaktieren.
  [Yes, Facebook is like a telephone book. I am pleased if people who are looking for me also can find me in order to contact me.] (no value)
- ○ Ja, ich bin froh, wenn ich unterschiedliche Informationen über die Welt, wie zum Beispiel Werbung, bekomme (z.B. per SMS).
  [Yes, I am pleased if I get different information about the world such as advertising.] (no value)
- ○ Nein, ich habe Angst, dass meine Telefonnummer für Werbung missbraucht wird.
  [No, I am afraid that my phone number will be misused for advertising.] (extrinsic value)

- Nein, ich habe Angst, dass ich belästigt oder bedroht werde.
  [No, I am afraid that I will be harassed or threatened.] (extrinsic value)
- Nein, das würde meine Privatsphäre verletzen und Privatsphäre ist etwas ganz wichtiges für mich.
  [No, that would violate my privacy and privacy is something very important for me.] (intrinsic value.)
- Andere Meinung: [Other opinion:]

F57: Ist es für dich ein Problem, wenn Fotos von dir, auf denen du betrunken bist und bei deren Betrachtung dies auch deutlich zu merken ist, auf Facebook öffentlich sichtbar sind? Was ist der wichtigste Grund, der dafür bzw. dagegen spricht?
[Q57: Do you mind if photos on which you are obviously drunk are publicly visible on Facebook. What is the most important reason for or against it?]

- Ja. Wenn solche Fotos von mir in der Öffentlichkeit auftauchen, dann ist das peinlich und ich schäme mich dafür.
  [Yes. If such photos are published it is embarrassing and I feel ashamed.] (extrinsic value)
- Ja. Ich habe Angst, dass mein Arbeitgeber oder ein zukünftiger Arbeitgeber diese Fotos sieht und ich dann Probleme in der Arbeit bekomme oder einen Job bei einem Bewerbungsgespräch nicht bekomme.
  [Yes. I am afraid that my employer or my future employer sees these photos and that I then get problems at work or will not get the job at an employment interview.] (extrinsic value)
- Ja. Das ist etwas Privates und Privatsphäre ist etwas ganz wichtiges für mich.
  [Yes. That is something private and privacy is something very important for me.] (intrinsic value)
- Nein. Ich habe kein Problem damit, auch Spaß muss sein im Leben und jeder ist mal betrunken, das ist völlig normal, man braucht so einen Umstand nicht zu verheimlichen.
  [No. I do not mind, there is no harm in a joke and everyone is drunk once in a time. This is completely normal. One does not need to conceal such a circumstance.](no value)
- Nein. Ich habe keine Angst mich so zu zeigen, wie ich bin. Selbst bei einem Bewerbungsgespräch kann das von Vorteil sein, da die Menschen sehen, dass man ein umgänglicher Mensch ist, der Spaß am Leben hat.
  [No. I am not afraid to show myself as I am. Even in an interview it can be a benefit, because people see that you are a sociable person that has fun in his/her life.] (no value)
- Andere Antwort: [Other opinion:]

F58: Würdest du jemals Bilder von dir, auf denen du nackt zu sehen bist, auf einem Social Networking Site Profil öffentlich machen? Was ist der wichtigste Grund, der dafür bzw. dagegen spricht?
[Q58: Would you ever publish pictures where you are shown naked on a social networking site profile? What is the most important reason for or against it?]

- Ja, warum nicht. Ich geniere mich nicht nackt vor anderen Menschen, auch nicht im Internet.
  [Yes, why not. I am not embarrassed being naked in front of other people, also not on the Internet.] (no value)
- Nein. Das wäre ein Eingriff in meine Intimsphäre. Intimität ist einer der wichtigsten Werte und muss geschützt werden.
  [No. That would be a violation of my privacy. Intimacy is one of the most important values and has to be protected.] (extrinsic value)
- Nein. Das ist zu privat und alle privaten Daten sollten privat bleiben und nicht öffentlich gemacht werden.
  [No. That is too private and all private data should be kept private and not be made public.] (intrinsic value)
- Andere Antwort: [Other opinion:]

F59: Social Networking Plattformen wie etwa Facebook oder Myspace zeichnen das Nutzungsverhalten ihrer User für Werbezwecke auf. Wie denkst du darüber?

(Mehrfachnennung möglich)
[Q59: Social networking platforms such as Facebook or Myspace record the usage behaviour of their users for purposes of advertising. How do you think about this circumstance? (multiple answers possible)]

- Das stellt für mich kein Problem dar. [I do not mind.] (no theory)
- Ich finde das schlecht und möchte selbst bestimmen können, welche Daten von mir aufgezeichnet werden.
  [I find that bad and I would prefer to decide for myself, which data are recorded about me.] (control theory)
- Ich finde das schlecht und denke, dass auf einer politischen Ebene Regeln gefunden werden sollten (z. B. Internationale Datenschutzregulierungen), die bestimmte Datensammlungen rechtlich unterbinden.
  [I find that bad and think that regulations should be established on a political level (e.g. international data protection regulations) in order to legally hinder the collection of certain data.] (access theory)
- Andere Meinung: [Other opinion:]

F60: In Österreich müssen Anbieter von Telekommunikationsdiensten (z.B. Internet Service Provider) elektronische Kommunikationsvorgänge ihrer Kunden auf Verlangen an die Polizei weitergeben. Siehst du darin ein Problem und wenn ja, wie könnte dem entgegengesteuert werden? (Mehrfachnennung möglich)
[Q60: In Austria, telecommunication service providers (e.g. Internet service providers) have to pass on electronic communication activities of their customers to the police if the latter demands so. Do you mind about it? If yes, how could this circumstance be counteracted? (multiple answers possible)]

- Nein, das stellt für mich kein Problem dar. [No, I do not mind.] (no theory)
- Ja, ich sehe das problematisch und würde gerne selbst bestimmen können, welche Kommunikationsvorgänge von mir weitergegeben werden.
  [Yes, I find that problematic and I would prefer to decide for myself, which communication activities of me can be passed on to the police.] (control theory)
- Ja, ich sehe das problematisch und denke, dass auf einer politischen, rechtlichen oder gesellschaftlichen Ebene Regeln gefunden werden sollten, die private Informationen schützen und niemand anderem zugänglich sind.
  [Yes, I find that problematic and I think that regulations should be established on a political, legal, or societal level in order to protect private information so that they are not accessible to someone else.] (access theory)
- Andere Meinung: [Other opinion:]

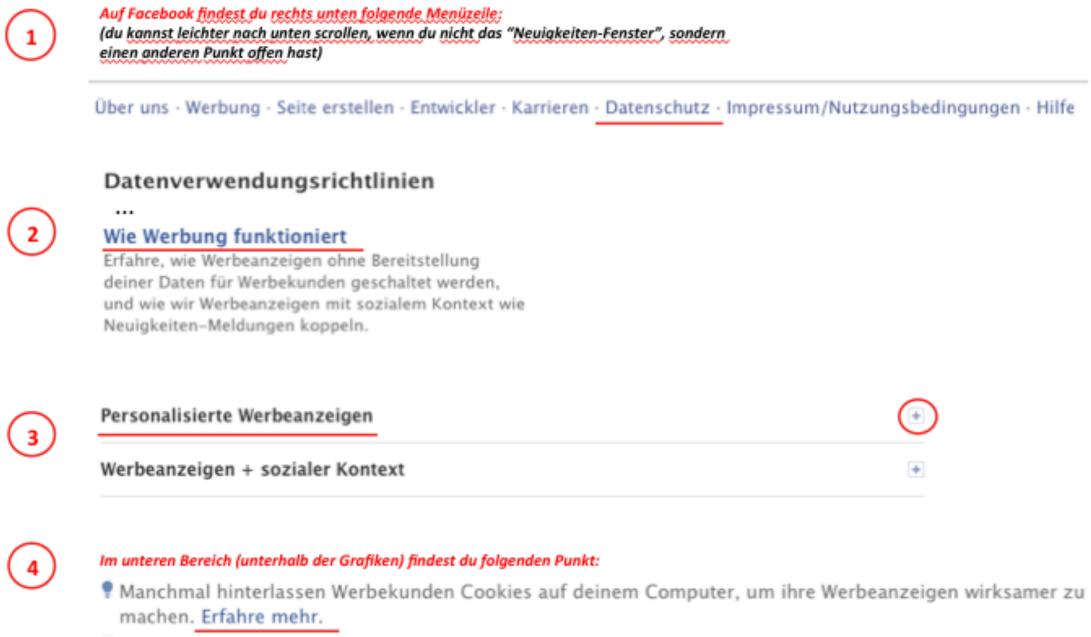
F61: Angenommen, du wirst auf Facebook von einer fremden Person wiederholt belästigt und du fühlst dich von diesem Menschen beobachtet (Stalking). Siehst du darin ein Problem und wenn ja, wie könnte eine derartige Situation gelöst werden? (Mehrfachnennung möglich)
[Q61: Suppose you are repeatedly harassed by a stranger on Facebook and you feel surveilled by this person (stalking). Do you mind about it? If yes, how could such a situation be handled? (multiple answers possible)]

- Nein, das stellt für mich kein Problem dar. (No, I do not mind.] (no theory)
- Ja, das stellt für mich ein Problem dar. Ich würde dieses Problem auf einer individuellen Ebene lösen, indem ich dieser Person den Zugang zu meinem Facebook Profil verwehre.
  [Yes, I mind. I would solve this problem on an individual level by denying this person access to my Facebook profile.] (control theory)
- Ja, das stellt für mich ein Problem dar. Ich würde mir wünschen, dass auf einer politischen, rechtlichen oder gesellschaftlichen Ebene Regeln gefunden werden könnten, die private Daten vor jedem Zugriff durch Andere schützen.
  [Yes, I mind. I wish that regulations could be established on a political, legal, or societal level in order to protect the access to private data.] (access theory)
- Andere Meinung: [Other opinion:]

Auf vielen Social Networking Sites werden Cookies platziert, welche es Werbetreibenden erlauben, die Wirksamkeit ihrer Werbeanzeigen zu messen oder Werbeinhalte nutzerspezifisch anzupassen.
Die "Network Advertising Initiative" ermöglicht es dir, diese Cookies zu deaktivieren.
[A lot of Social Networking Sites use cookies, in order to allow advertisers to measure the impact of a campaign or to personalise an advertisement.]

Auf Facebook findest du in den Datenschutzrichtlinien einen Link zur Homepage von www.networkadvertising.org.
Diese Seite kannst du auch direkt aufrufen unter:
http://www.networkadvertising.org/managing/opt_out.asp

[On Facebook within the privacy policy you can find a link to the homepage of www.networkadvertising.org. You can also directly visit it under http://www.networkadvertising.org/managing/opt_out.asp]



1 *Auf Facebook findest du rechts unten folgende Menüzeile:*
(du kannst leichter nach unten scrollen, wenn du nicht das "Neuigkeiten-Fenster", sondern einen anderen Punkt offen hast)

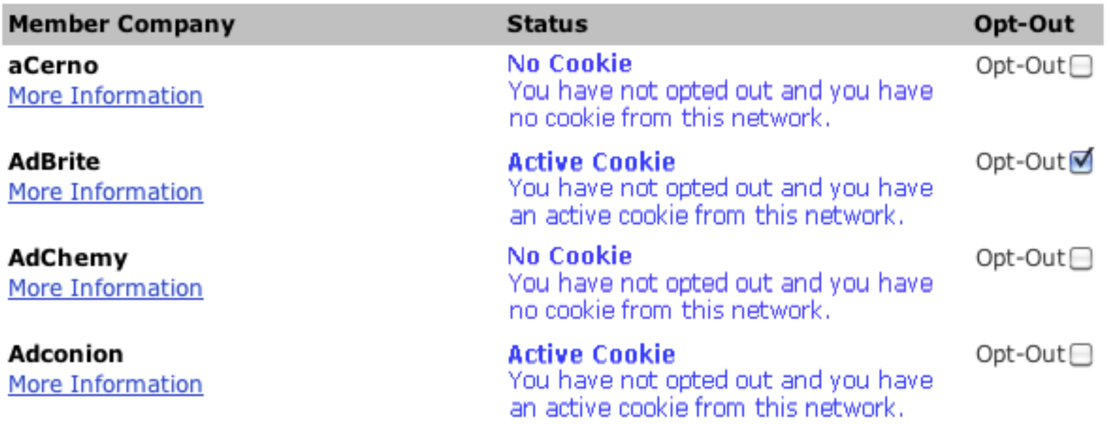
Über uns · Werbung · Seite erstellen · Entwickler · Karrieren · Datenschutz · Impressum/Nutzungsbedingungen · Hilfe

2 Datenverwendungsrichtlinien
...
Wie Werbung funktioniert
Erfahre, wie Werbeanzeigen ohne Bereitstellung deiner Daten für Werbekunden geschaltet werden, und wie wir Werbeanzeigen mit sozialem Kontext wie Neuigkeiten-Meldungen koppeln.

3 Personalisierte Werbeanzeigen +
Werbeanzeigen + sozialer Kontext +

4 *Im unteren Bereich (unterhalb der Grafiken) findest du folgenden Punkt:*
Manchmal hinterlassen Werbekunden Cookies auf deinem Computer, um ihre Werbeanzeigen wirksamer zu machen. Erfahre mehr.

Auf der Website der Network Advertising Initiative hast du die Möglichkeit aus einer Liste von Werbeunternehmen diejenigen zu identifizieren, welche auf deinem Computer ein aktives Cookie platziert haben. Du kannst für jedes einzelne Cookie bestimmen ob du es deaktivieren willst, indem du "Opt-Out" wählst.
[This Website of the Network Advertising Initiative allows you to identify from a list of advertisers those that placed a Cookie on your computer. For each Cookie you can define, if you want to deactivate it by choosing "Opt-Out".]



Member Company	Status	Opt-Out
aCerno More Information	**No Cookie** You have not opted out and you have no cookie from this network.	Opt-Out □
AdBrite More Information	**Active Cookie** You have not opted out and you have an active cookie from this network.	Opt-Out ☑
AdChemy More Information	**No Cookie** You have not opted out and you have no cookie from this network.	Opt-Out □
Adconion More Information	**Active Cookie** You have not opted out and you have an active cookie from this network.	Opt-Out □

[Q62: Have you known about this possibility to deactivate Cookies?]

○ Ja [Yes]
○ Nein [No]
○ Ich weiß nicht [I don’t know]

F63: Hast du über Facebook, eine andere Website, oder auch direkt, schon einmal die Site von www.networkadvertising.org besucht?
[Q63: Have you ever visited www.networkadvertising.org via Facebook, any other website or even directly?]

○ Ja [Yes]
○ Nein [No]
○ Ich weiß nicht [I don’t know]

(Verzweigungslogik: nur angezeigt, wenn bei S32_F63 „ja“)
[Question logic: only displayed if Q63: “yes”]

F64: Nutzt du die Möglichkeit mittels der "Network Advertising Initiative" Cookies auf deinem Computer zu blockieren?
[Q64: Do you take advantage of the opportunity to block cookies on your computer through the “Network Advertising Initiative”?]

○ Ja [Yes]
○ Nein [No]
○ Ich weiß nicht [I don’t know]

(Verzweigungslogik: nur angezeigt, wenn bei S33_F64 „nein“ oder „weiß nicht“)
[Question logic: only displayed if Q64: “no”/ “I don’t know”.]
F65: Willst du zukünftig mit Hilfe der Network Advertising Initiative Werbeunternehmen daran hindern, Cookies auf deinen Computer zu platzieren?
[Q65: In the future, will you prevent advertisers from placing cookies on your computer through the Network Advertising Initiative?]

○ Ja [Yes]
○ Nein [No]
○ Ich weiß nicht [I don’t know]

Abschließend bitten wir dich noch um ein paar Angaben zu deiner Person:
(Zutreffendes bitte ankreuzen bzw. ausfüllen)
[Finally, we ask you for some information about yourself (please check the appropriate box or fill in).]

F66: Dein Geschlecht:
[Q66: Your Sex:]

- ○ weiblich [female]
- ○ männlich [male]

F67: Wie alt bist du?
[Q67: How old are you?]

Bitte gib hier die Zahl ein:
[Please fill in the the number:]

F68: An welcher Universität studierst du?
(Solltest du mehrere Studien absolvieren, die folgenden Fragen bitte für dein Hauptstudium beantworten)
[Q68: Which university do you attend? (Should you be enrolled in more than one field of study, please answer the following questions for the main one).]

Bitte wähle aus der Liste aus:
[Please choose from the list:]

Universität Wien
Wirtschaftsuniversität Wien
Technische Universität Wien
Medizinische Universität Wien
Universität für Bodenkultur Wien
Veterinärmedizinische Universität Wien
Universität für angewandte Kunst Wien
Universität für Musik und darstellende Kunst Wien
Akademie der bildenden Künste Wien
Universität für Weiterbildung Krems
Universität Graz
Technische Universität Graz
Medizinische Universität Graz
Universität für Musik und darstellende Kunst Graz
Montanuniversität Leoben
Universität Linz
Universität für künstlerische und industrielle
Gestaltung Linz
Universität Salzburg
Universität Mozarteum Salzburg
Universität Klagenfurt
Universität Innsbruck
Medizinische Universität Innsbruck

F69: In welchem Studienabschnitt befindest du dich?
[Q69: What is your level of study?]

- ○ Bachelor/Bakkalaureat [Bachelor]
- ○ Master/Mag/DI [Master]
- ○ Doktorat [PhD]
- ○ Diplomstudium [Diploma Study]
- ○ Sonstiges (bitte angeben) [Other (please state)]

F70: Wie viele Semester hast du bereits studiert? (inkl. SS 2011)
[Q70: How many semesters have you already studied? (including summer term 2011)]

Bitte gib hier die Zahl an:
(Please fill in the number:)

F71: Du bist Student/in der:
(Q71: Your field of study is:)

- o Naturwissenschaften [Natural Sciences]
- ○ Technische Wissenschaften, Ingenieurswissenschaften [Technical or Engineering Sciences]
- o Sozialwissenschaften [Social Sciences]
- o Wirtschaftswissenschaften [Economics]
- o Geistes- und Kulturwissenschaften [Humanities and Cultural Studies]
- o Kunst [Arts]
- o Theologie [Theology]
- o Rechtswissenschaften [Law]
- o Medizin [Medicine]
- o Land- & Forstwissenschaften, Veterinärmedizin [Agricultural Sciences and Veterinary Medicine]
- o Sport [Sports]
- o Sonstiges (bitte angeben) [Other (please state)]

(Verzweigungslogik: nur angezeigt, wenn bei S35_F71 „technische wissenschaften/ingenieurswissenschaften")
*(Question logic: only displayed, if Q71: "*Technical or Engineering Sciences")
F72: Bist du Student/in der Informatik/Computerwissenschaften?
[Q72: Do you study Computer Science?]

- o Ja [Yes]
- o Nein [No]

F73: Wie viel Geld steht dir im Monat zur Verfügung (inkl. aller Einkommen, Stipendien, Beihilfen, Unterstützung durch deine Eltern, usw.)?
[Q73: What is your average monthly income (including subsidies your receive by your parents, the state or grants).]

- o weniger als 400 € [less than 400€]
- o 401 - 600€
- o 601 - 800€
- o 801 - 1.000€
- o 1.001 - 1.200€
- o 1.201 - 1.400€
- o 1.401 – 1.600€
- o 1.601 – 1.800€
- o 1.801 – 2.000€
- o über 2.000 € [more than 2.000€]

F74: Arbeitest du neben deinem Studium?
Wenn ja, in welchem Ausmaß (im Durchschnitt/Woche)?
[Q74: Do you work in addition to studying? If yes, approximately how many hours a week?]

- o Nein [No]
- o Ja, aber sehr unregelmäßig (zb. nur in den Ferien als Ferialkraft)
  [Yes, but only sporadic (e.g. only during holidays)]
- o Ja, bis zu 10 Stunden [Yes, up to 10 hours]
- ○ Ja, bis zu 20 Stunden [Yes, up to 20 hours]
- o Ja, bis zu 30 Stunden [Yes, up to 30 hours]
- o Ja, mehr als 30 Stunden [Yes, more than 30 hours]

(*Verzweigungslogik: nur angezeigt, wenn bei S37_F74 eine „ja"-option gewählt wurde)*
[Question logic: only displayed, if Q74 "yes"]
F75: Warum arbeitest du zusätzlich zum Studium? (Mehrfachnennung möglich)
[Q75: Why do you work in addition to studying? (multiple answers possible)]

- o um mir mein Studium/Leben finanzieren zu können.
  [to afford my studies/life.]
- o um zusätzlich etwas mehr Geld zur Verfügung zu haben (z.B. Shopping, Reisen).
  [to have some additional money at hand (e.g. for shopping, travel).]
- o um Berufserfahrung zu sammeln.
  [to gain some work experience.]
- o weil ich im Rahmen meines Studiums Pflichtpraktika absolvieren muss.

[because within my study programme I'm obliged to complete an internship.]

- ○ aus persönlichem Interesse bzw. Spaß.
  [out of personal interest & pleasure.]
- ○ weil ich andere mitfinanzieren muss.
  [because I have to co-finance others.]
- ○ Sonstiges (bitte angeben)
  [Other (please state)]

F76: Welchen höchsten Schulabschluss haben deine Eltern?
[Q76: What is the highest educational achievement of your parents?]

	Vater [Father]	Mutter [Mother]
Pflichtschule/ kein Abschluss [Compulsory no school-leaving qualification]	□	□
Lehre [vocational training]	□	□
Berufsbildende mittlere Schule, Fachschule (ohne Matura) [Middle School, technical college (without A-levels)]	□	□
Meisterprüfung [master craftsman's examination]	□	□
Matura [High School Diploma]	□	□
Akademie (PädAK, SozAK) [academy]	□	□
Universität, Hochschule [university/college]	□	□
weiß nicht [I don't know]	□	□

F77: Welchen Berufsstatus haben bzw. hatten deine Eltern hauptsächlich?
[Q77: What is or was the general occupational status of your parents?]

	Vater [Father]	Mutter [Mother]
ArbeiterIn [blue collar worker]	□	□
Angestellte/r oder Beamter/in ohne Leitungsfunktion [white collar employee or civil servant without responsibility for personnel]	□	□
Angestellte/r oder Beamter/in mit Leitungsfunktion [white collar employee or civil servant in a leadership role]	□	□
FreiberuflerIn [freelancer]	□	□
KleinunternehmerIn/UnternehmerIn ohne Angestellte [small businessman/entrepreneur without employees]	□	□
UnternehmerIn, Gewerbetreibende/r mit Angestellte [entrepreneur/trader with employees]	□	□
LandwirtIn, ForstwirtIn [farmer, forest worker]	□	□
mithelfend im Betrieb [assisting in the family business]	□	□

	Vater [Father]	Mutter [Mother]
war nie erwerbstätig [has never been gainfully employed]	□	□
weiß nicht [I don’t know]	□	□

Vielen Dank für die Teilnahme an der Studie! Deine Antworten sind für uns hilfreich, um die Forschungsarbeit zu Social Networking voranzutreiben.

Wenn du an der Verlosung von den Amazongutscheinen teilnehmen möchtest, dann gib bitte deine E-Mail-Adresse ein. Diese wird unabhängig von deinen Antworten verarbeitet.

Wenn du Updates über Forschungsberichte, die aus diesem Projekt resultieren, erhalten möchtest, gib bitte deine E-Mail-Adresse an.

F78: Du kannst das Feld auch unausgefüllt lassen.

- ○ Teilnahme am Gewinnspiel
- ○ Infos über Forschungsberichte erhalten
- ○ Keine Angabe
- ○ E-Mail-Adresse:

Die GewinnerInnen der Gutscheine werden nach Abschluss der Umfrage zufällig gezogen und per E-Mail verständigt.

Wir würden uns freuen, wenn du deine StudienkollegInnen, die ebenfalls Social Networking Plattformen benutzen, auf die Umfrage hinweist:

https://www.surveymonkey.com/s/social_networking_sites

[Thank you for participating in this study. Your answers are important for us in order to advance research about social networking.
If you want to take part in winningone of the Amazon vouchers, then please enter your email address. It will be stored independently of your answers.
If you want to receive updates on research reports that result from this project, then enter your email address.
Q78: You can leave the following field blank.

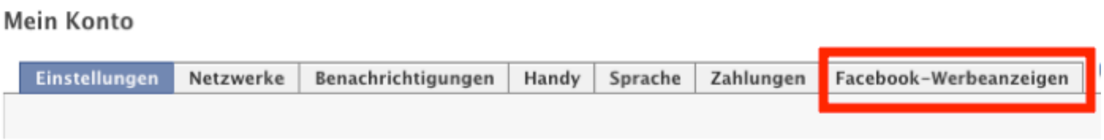
- participate in the lottery
- receive information on research reports
- not specified
- email-address:

The winners of the vouchers are drawn randomly after the survey ends. They will be notified per email.
We are happy if you inform your friends and colleagues that also use social networking platforms about this survey:
https://www.surveymonkey.com/s/social_networking_sites]

Screenshots alt: [changed Screenshots:]

Auf **Seite 20** >> Zweiter Screenshot wurde am 18. August auf neues Facebook Screendesign umgestellt. Vormalige Version siehe unten:
[Site 20: second screenshot needed to be adapted to Facebook’s new screendesign

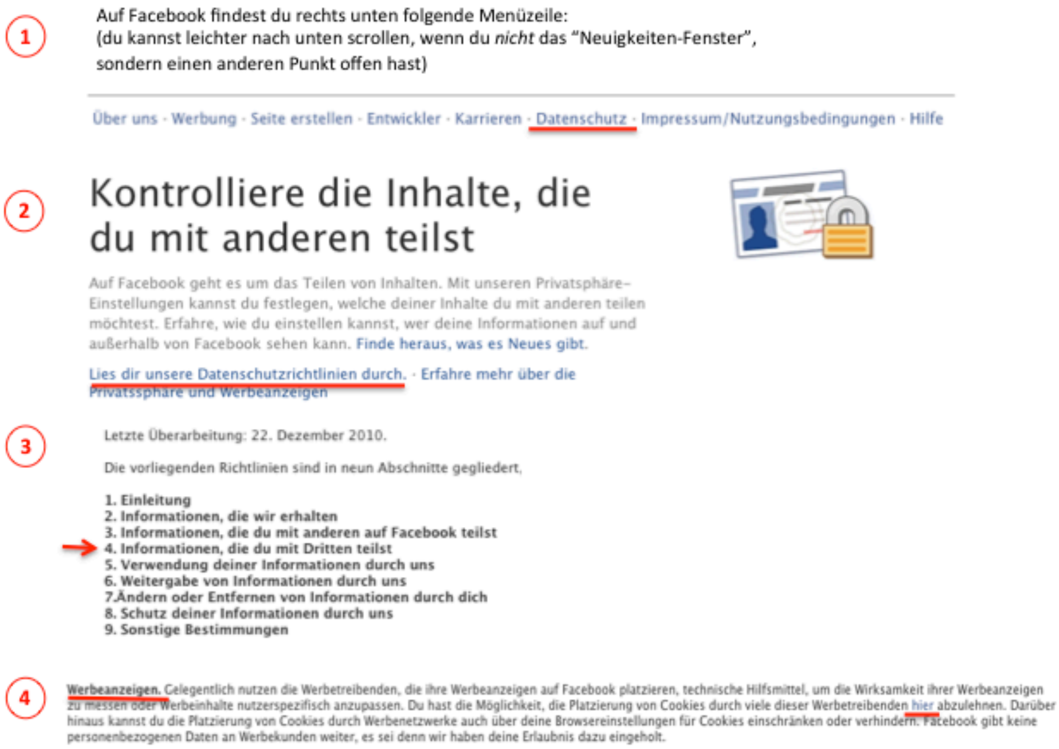
(18.08.2011). former version below:]



Mein Konto

Auf **Seite 32** >> Link zur Advertising Network Initiative vor 07.September 2011 noch zu finden mittels folgender Anleitung:

[Site 32: After 7th September, due to changes the link tot he Advertising Network Initiative was harder to find. Before it could have been found by following these four steps:]



1 Auf Facebook findest du rechts unten folgende Menüzeile:
(du kannst leichter nach unten scrollen, wenn du *nicht* das "Neuigkeiten-Fenster",
sondern einen anderen Punkt offen hast)

Über uns · Werbung · Seite erstellen · Entwickler · Karrieren · Datenschutz · Impressum/Nutzungsbedingungen · Hilfe

2 Kontrolliere die Inhalte, die du mit anderen teilst

Auf Facebook geht es um das Teilen von Inhalten. Mit unseren Privatsphäre-Einstellungen kannst du festlegen, welche deiner Inhalte du mit anderen teilen möchtest. Erfahre, wie du einstellen kannst, wer deine Informationen auf und außerhalb von Facebook sehen kann. Finde heraus, was es Neues gibt.

Lies dir unsere Datenschutzrichtlinien durch. · Erfahre mehr über die Privatssphäre und Werbeanzeigen

3 Letzte Überarbeitung: 22. Dezember 2010.

Die vorliegenden Richtlinien sind in neun Abschnitte gegliedert,

1. **Einleitung**
2. **Informationen, die wir erhalten**
3. **Informationen, die du mit anderen auf Facebook teilst**
4. **Informationen, die du mit Dritten teilst**
5. **Verwendung deiner Informationen durch uns**
6. **Weitergabe von Informationen durch uns**
7. **Ändern oder Entfernen von Informationen durch dich**
8. **Schutz deiner Informationen durch uns**
9. **Sonstige Bestimmungen**

4 **Werbeanzeigen.** Gelegentlich nutzen die Werbetreibenden, die ihre Werbeanzeigen auf Facebook platzieren, technische Hilfsmittel, um die Wirksamkeit ihrer Werbeanzeigen zu messen oder Werbeinhalte nutzerspezifisch anzupassen. Du hast die Möglichkeit, die Platzierung von Cookies durch viele dieser Werbetreibenden hier abzulehnen. Darüber hinaus kannst du die Platzierung von Cookies durch Werbenetzwerke auch über deine Browsereinstellungen für Cookies einschränken oder verhindern. Facebook gibt keine personenbezogenen Daten an Werbekunden weiter, es sei denn wir haben deine Erlaubnis dazu eingeholt.