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 Three

Author: Sebastian Sevignani

Research Paper Number #14

Date of Publication: December 24, 2012

Author Institution: Unified Theory of Information Research Group (UTI)

Author Address:

Author e-Mail: sebastian.sevignani@uti.at

Author URL: http://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

FWF Der Wissenschaftsfonds.

SN[S]³ Social Networking Sites in the Surveillance Society

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

Sebastian Sevignani

Keywords: critical theory, critical methodology, qualitative interview study, privacy, surveillance, targeted advertising, social networking sites, alienation, exploitation, alternative social networking sites, privacy trade-offs, private property, commodification

Short biography of the author/s: Sebastian Sevignani studied media and communication, philosophy, and theology at the University of Salzburg. He obtained a master's degree in communication studies in 2009. From 2007 until 2010, he worked at the University of Salzburg's Department of Communication Studies as a scholar in the Media Economics Research Group. His doctoral thesis focuses on the political economy of privacy in informational capitalism. Sebastian is a member of the Unified Theory of Information Research Group (UTI) and of the working group "Public Policy and the Regulation of Surveillance" of the European Cooperation in Science and Technology Action "Living in Surveillance Societies (COST Action IS0807)". He is a member of the editorial team of tripleC: Journal for a Global Sustainable Information Society.

A general advice that is given in the methodological literature is to make clear what position the research comes from (not at least because it influences the validity of empirical data). We assume that this deserves even more attention in the context of qualitative research because the methodological field of qualitative research is characterized by a plethora of different positions: "Qualitative research methods is a complex, changing and contested field – a site of multiple methodologies and research practices [...] Three aspects of this diversity concern paradigms, approaches to data, and methods for the analysis of data" (Punch 2005, 134). We will discuss these points in the following sections (sections 2-3), before we present results (section 4), and discuss limitations of our study, which also point to suggestions for further research (section 5) .

1. Research paradigm and methodology

We study surveillance and privacy on social networking sites (SNS) within a critical approach that borrows from Marxian analysis of capitalist society and its further development, for instance by Frankfurt School theorists. Our paradigmatic position comes close to the "conflict paradigm" (Babbie 2010, 36) and a "demystification framework" (Punch 2005, 138; Reinharz 1992, 191-194): "Critical theory wants to explain a social order in such way that it becomes itself the catalyst which leads to the transformation of this social order" (Fay 1993, 33). In our context, this means we want to explain surveillance on SNS in such a way that it becomes itself a catalyst which leads to a social situation of fully realized user privacy. Fully realized privacy would allow collective and individual self-determination. Our research wants to enlighten and empower SNS users in that sense. Critical research, as we understand it, is based on several assumptions (Fay 1993):

- structural conflicts are underlying society,
- those conflicts advance suffering among a majority of the society's members and constitute a crisis,
- and the majority of society's members shows ignorance or has false consciousness of the structural conflicts.

Capitalist profit interests broadly determine the Internet and SNS (Fuchs 2008). These interests can contravene users' needs to communicate and collaborate insofar as those needs can only be satisfied if they do not inhibit profit. In principle users' needs are of secondary importance. Such conflicts are expressed in the well documented crisis of privacy in the digital age. However, a majority of SNS users are less conscious of the origins of the most important privacy threats. We think that those threats mainly rest with economic surveillance and states' interest in order to control citizens. The latter is not our thematic priority; rather economic surveillance that means collecting, storing and processing of user/consumer data for economic purposes.

Nowadays SNS are mainly commercially organised. Commercial SNS are steadily under pressure to gain profits. Their profit strategy is mainly based on the targeted advertising business model, which means that they engage in exchange contracts with the advertising industry. The SNS owner buys technical infrastructure, such as server parks and software components, as well as labour force, such as accountants, software developer, etc, and produces the SNS on which users can interact. While people use the site for different reasons, such as getting news, providing information, staying in touch with friends, making new relations, or organising events, they produce a wide range of data. These data, which include for instance socio-demographic information and consumer preferences deduced from users' browsing behaviour, are then sold to advertisers. Whereas traditional forms of advertising are directed to broad groups of potential buyers, targeted advertising is tailored for exactly defined and differentiated groups, or even single consumers. This demands more detailed, exact, and differentiated knowledge of the users' needs and (buying) behaviour, which can be provided by the owner of SNSs. The SNSs' business model is based on the secondary use of user interactions for profit purposes. The economic reason why profit-oriented SNSs develop massive systems of user surveillance and store 'literally everything', as a employee of the most popular SNS Facebook once has admitted, lies therein. SNS' terms of use and privacy statements allow the widespread collection, storage, and assessment of personal data and support the targeted advertising business model (Sandoval 2011; Fernback and Papacharissi 2007, 730). The status quo situation and the status quo revenues are insufficient for dominant SNS, such as Facebook, and its potential investors; it naturally plans therefore to extend advertising in order to increase profits.

Why should we be critical of SNS that are structurally based on surveillance? When we think about this question we have to shed light on the social conditions that give birth to power asymmetries on SNS. In particular Fuchs (2010b; 2010c; 2011c; 2011d; 2012) stresses the importance of exploitation processes that are taking place on SNS. Most generally exploitation is the structural appropriation of societal produced surplus. Thereby one societal group profits more from the achievements of another group than the latter group itself is able to profit from their own achievements. Conceptualising "achievements" as fruits of labour, Marx argues: "Wherever a part of society possesses the monopoly of the means of production, the worker, free or unfree, must add to the labour-time necessary for his own maintenance an extra quantity of labour-time in order to produce the means of subsistence for the owner of the means of production" (Marx 1867/1976, 344). In capitalism, the exploitation of this surplus or extra working time takes on a "more refined and civilized" (486) form. This is because work force becomes an exchangeable commodity that is now traded on the labour market. A person will only trade his workforce, when "a complete separation between the workers and the ownership of the conditions for the realization of their labour" (874) is established in society. Exactly that was the case when capitalism arose; Marx refers to the process of separation as "primitive accumulation of capital" and describes it as a violent process of expropriation of great segments of the

population (Marx 1867/1976, part eight). In consequence, the labourer received a twofold freedom (270-272), namely henceforth workers are free of personal dependences, for instance, from their overlords in feudalism, but also free from the ownership of the condition for the realisation of their labour. Workers are on the one hand free to engage in contracts, which is precisely the freedom of commodity exchange. On the other hand, workers are forced to engage in contracts and to sell their labour power on the markets to make ends meet. This freedom is also set in commodity exchange as it is a freedom to choose regardless of one's social status. Hence, workers are forced to maintain their status as a subaltern class because the capitalist can steadily appropriate the societal surplus that is produced by the workers (729-730). This "freedom based", "fair", "civilised", and "more refined" capitalist exploitation process is, according to Marx, a structural reason for domination in society. The capitalist quality of society as class society is ultimately expressed by the right to have others work for you and the right to private property in labour's terms of realisation that enable structural exploitation. Within critical political economy of the media, Dallas Smythe (1977), discussed how exploitation works in the realm of media. He speaks of the commodification of audiences through the corporate media (1977, 3). Just like the labour power was commodified and became exchangeable on markets with the rise of capitalism, the audience power is now traded in the media industry. Whereas Smythe's focus was more on the media institutions, which are producing audience commodities, Jhally and Livant (1986), taking Smythe's analysis as a starting point, focus on the audience activity within the process of audience commodification. They refer to this activity as "watching as working" or the "work of watching" and point out commonalities to the labour process: Watching "is a human activity through which human beings relate to the external physical world and to each other" (126); and „while workers sell labor-power to capitalists, audiences sell watching-power to media owners; and as the use-value of labor-power is labor, so the use-value of watching-power is watching, the capacity to watch" (135). Capitalist media try to increase the efficiency of the work of watching: "the central problem for the media is not simply to get people to watch but to get them to watch extra. The problem for the commercial media is to maximize the production of this commodity and to attempt to minimize the costs of doing so" (126). In analogy to Marx's analysis (Marx 1867/1976, part three and four), Jhally and Livant see two basal opportunities for the media to achieve this: On the one hand, the „attempt to expand total advertising time" (Jhally and Livant 1986, 133). Facebook's introducing of advertisements for mobile phones, is a corresponding example. On the other hand, media attempt to „make the time of watching advertising more intense - they can make the audience watch harder" (133). An example for that is targeted advertising to avoid scattering losses. Mark Andrejevic (2002) consequently makes use of these ideas to explain exploitation processes that are typical for social media. Andrejevic argues that, within the "surveillance-driven culture production" (Turow 2005, 113), there is a new form of working involved additionally to the work of watching: "The labor of being watched goes hand-in-hand with the work of watching: viewers are monitored so advertisers can

be ensured that this work is being done as efficiently as possible“ (Andrejevic 2002, 236). Commercial SNS's focus, on behalf of surveillance technologies, on the exploitation of “content about the content“ (Andrejevic 2011, 284), that is exploiting data about user interactions.

We further propose to think of the previous discussed user exploitation and its manifest problems as a particularising objectification of the broader philosophical category of alienation. In Marx, alienation, which he has found as a general philosophical idea in Hegel, becomes a critical concept when he applied it to the concrete historical formation of capitalist society (Dyer-Whiteford 2010, 487). According to Marx, alienation is given in capitalism as producers cannot self-determine about the circumstances of the realisation of their labour force and therefore cannot recognise themselves in their work and the products they have made. In the Economic and Philosophical Manuscripts (1844/1988), Marx speaks about four forms of alienation focussing on labour: First, the producer is alienated from his product (product alienation); he has no control over the things that he is producing. Second, the worker is alienated from the processes wherein he produces things (process alienation). He then speaks about consequences of alienated labouring for, third, the self (self-alienation) and, fourth, for society (societal alienation). Self-alienation and societal alienation, broadly speaking, means that in capitalism, man-made things exercise force over man (Haug 2005, 161). That is, on the one hand, that the individual is other-directed and not in control over his or her life, and on the other hand, individuals together are societally alienated if they cannot consciously shape the society within they would like to live in (see Comor 2011, 318). As mentioned before, exploitation and alienation are interwoven: “A further test of exploitation is whether a form of appropriation results in the return of the fruit of one's own labor in the form of an alien force“ (Andrejevic 2010, 95). If one class has the opportunity to appropriate societal produced surplus and becomes richer and more powerful then they has also the power to set working conditions within which product and process alienation are dominant. On the other hand, contrary to Mark Andrejevic, who tends to blur the differences between the two concepts (2010, 94; 2011, 284, 286), Marx makes clear that there is a difference between alienation and exploitation. He argues, that “the propertied class and the class of the proletariat present the same human self-alienation. But the former class finds in this self-alienation its confirmation and its good, its own power: it has in it a semblance of human existence. The class of the proletariat feels annihilated in its self-alienation; it sees in it its own powerlessness and the reality of an inhuman existence“ (Marx 1844 in McLellan 2000, 148). All humans in capitalism are alienated, however the exploited are in particular suffering from this alienation. It is an ongoing matter of dispute whether alienation and its various aspects are obsolete or still relevant in the realm of SNS. Eran Fisher (2012) argues that there is indeed less alienation on SNS, and he refers in particular to product and process alienation: He says, that “less alienation refers to a greater possibility to express oneself, to control one's production process, to objectify one's essence and connect and communicate with others“ (173) but he also adds, that less alienation in turn creates

more exploitation for the users. A similar argument is made by Rey (2012); he sees alienation in decrease, whereas exploitation remains relevant in the realm of social media. Coercion is one aspect frequently associated with alienation. Campbell and Carlson observe that SNS users "cooperate in the online gathering of data about themselves as economic subjects" (2002, 588) and engage in self-surveillance. Such self-surveillance seems to refer to indirect and mediated forms of coercion and to alienation ultimately. Campbell and Carlson (590-591) however reflect that unlike from the panoptic prison where "self-surveillance" and "self-disciplining" is protected and fostered by external and direct coercion, on SNS no such obvious coercion exists. In that context Andrejevic contends that "coercion is inscribed into the social relations themselves" (Andrejevic 2011b, 283); and that it is objectified in the control over productive resources. Social media are "the privately owned means of sociality" (2011a, 93), that provide owners with the power to set the terms of access to them. It is crucial for critical theory to strictly differentiate between the access to the means of sociality and communication, on the one hand, and control respectively ownership over these means, on the other hand (97). One can add the importance to further differentiate between formal ownership and real control because, we can observe that on SNS users remain "full ownership" of their data, but grant the SNS excessive control permissions. Focusing on these structural aspects, Comor (2011) is clear regarding the question of alienation. He says that "prosumption's 30-year ascent appears to be more about power's centralization than decentralization; more about the furtherance of hierarchy than its retreat; more about the perpetuation of alienation than a mechanism for self-realization and genuine freedom" (321).

Notable problems of produser alienation and exploitation on SNS are, for instance, the following: Owners of SNS, not their users are determining the conditions of online social networking. They develop complex and often confusing terms of use and privacy policies that allow them to surveil and to which users can hardly give an informed consent. Additionally to a lack of self-determination produsers also face constrained decisional freedom. If they want to use SNS they have to consent to terms that offer only a limited range of decision opportunities. An opt-out opportunity for advertising does not appear in the privacy setting options as it would contradict SNS's subject matter. We can assess that there is a lack of democracy concerning SNS as even the majority of produsers cannot determine the conditions within which they interact and communicate. Economic surveillance, identification, classification, and assessment of user data for targeted advertising purposes also lacks democratic control as these processes are mainly in-transparent for users that have no access to advanced technological skills or business plans, which are kept secret by commercial SNS. When using commercial SNS, produsers cannot escape advertising. Sponsored products, services, and ideological campaigns come together with chatting, mailing with friends. This subtle way, interests of advertisers can influence produsers thinking and acting more likely that products, services, and ideas that cannot afford advertising can do. Power asymmetries, hence market concentration, manipulation of needs, intransparency, lack of democracy, self-determination, and decisional freedom are

grounded in and reproduced through exploitation processes. Owners of SNS are able to privately appropriate and utilise commonly produced information and interactions. They extend profit logics to further spheres of life.

In contrast to our critical analysis, public discussion and SNS users' concerns are mainly not about economic surveillance and profit interests, rather they are about privacy. However, discussions about privacy partially deflect from structural conflicts underlying the Internet and society (Lyon 1994, 197). They also work as an ideology in favour of the status quo that is characterised by economic surveillance and profit interests. This is because the dominant concept of privacy, which is urged as an argument against surveillance by many, is itself a motive of surveillance. A closer analysis shows that the poles of the opposing pair of privacy and surveillance are interconnected, insofar as both are related to private property in capitalism (Figure 1). Our theory is consistent with observations by others: "A society of strangers is one of immense personal privacy. Surveillance is the cost of that privacy" (Nock 1993, 1), and "in our nomadic world the society of strangers seeks privacy that actually gives rise to surveillance" (Lyon 2005, 27). According critical theory "the conception of the contradictory nature of societal reality does not, however, sabotage knowledge of it and expose it to the merely fortuitous. Such knowledge is guaranteed by the possibility of grasping the contradiction as necessary and thus extending rationality to it" (Adorno 1976c, 109).

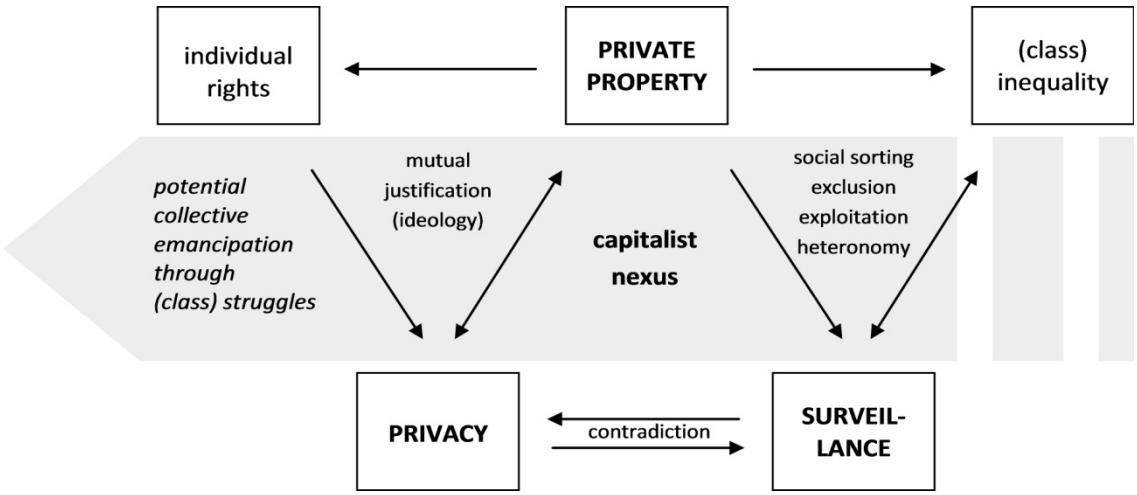

Figure 1: Critical political economy of surveillance and privacy framework

State protected private property in the means of production enables exploitation, gives rise to social inequality of power, and constantly reproduces a society, which is structurally divided into classes. It is the basis for companies' profit seeking and market competition. So it necessitates both, controlling, property protecting, and security guaranteeing state surveillance as well as economic surveillance. Economic surveillance, as we stated before, is a frequently applied business model in the Internet. Macpherson (1978a; b) has described how property necessarily becomes identified with private property in capitalism, which is essentially the right to exclude others.

A resemblance between privacy and property is often noted in the literature (Lyon 1994, 186; Laudon 1996, 93; Brenkert 1979, 126; Habermas 1991, 74; Goldring 1984, 308-309; Lessig 2002, 250; Hettinger 1989, 45; Geuss 2001, 103; Sofsky 2007, 95-96; Solove 2009, 26-28; Moore 2008, 420; Kang 1998; Litman 2000; Westin 1967, 324-325; Varian 1997; Samuelson 2000). Several authors (Fuchs 2011c; Sevignani 2012; Lyon 1994, 186; Allmer 2011) have argued that the dominant notion of the value of privacy is a possessive individualistic one. In accordance with the liberal worldview (see recently Sofsky 2008), people refer to "the owner's privacy against invasion" (Mill 1965, 232) of others. Possessive individualism denotes a kind of thinking and a social practice. Within capitalism it is useful and necessary that the individual perceives herself or himself as essentially "the proprietor of his own person and capacities, for which he owes nothing to society" (Macpherson, 1962, 263) and enters "into self-interested relations with other individuals" (Macpherson 1962, 263). Sevignani (2012) argues that the demand for privacy as individual control over personal data is heavily linked to the mutual recognition of private property owners. Privacy, the supposed opponent of surveillance, is also traditionally connected to the justification of private property and capitalist social order (Mill 1965, 232; 938; Lyon 1994, 196; Macpherson 1962, Marx 1972, 235; Fuchs 2011c; Sevignani 2011). Our political economy analysis of surveillance and privacy shows a shared ground between them.

Critical research aims at emancipation from that social situation, which has not only evoked privacy crisis but also social inequality and heteronomy through social sorting, exclusion, and exploitation. It reflects and contributes to (class) struggles against surveillance and the exclusion of many from the means of production. In figure 1 this is expressed by the underlying grey arrow, which symbolise a move from the capitalist nexus of privacy and surveillance to the left side. Our research interest wants to leave behind a class society and seeks to establish fulfilled privacy and individual rights without a connection to capitalist private property by applying several critiques (Fay 1993, 36):

- "a critique of the self-understandings of the members of its audience;
- an explanation of why these self-understandings, though in some sense false, continue to be employed by these members;
- an account of why these understandings now can be undermined and how this specifically be done in present circumstances;
- an alternative interpretation of the identity – the capacities and real interests – of this audience;
- a demonstration the crisis nature of the workings of the society under discussion;
- and an identification of those aspects of this society which need to be changed if the crisis is to be resolved in a positive way for its audience."

We therefore want to study SNS users in four ways:

- As informants, by asking in which way surveillance and privacy issues are relevant to users of SNS.
- As participants of an ideological discourse by identifying and explaining the mutual justifications between private property, individual rights, surveillance, and privacy.
- As socially sorted, excluded, exploited, and other-directed people by the means of economic surveillance.
- As emancipator actors; in this context we are looking for users' arguments or feelings, which are directed to alternatives to surveillance and towards a collective and emancipatory Internet.

Our paradigmatic position corresponds with methodological considerations (thereby methodology is not methods; rather it refers to the overall study of how research proceeds). The image of our critical methodology becomes clear when it is opposed to positivism (Adorno et al. 1976).

"Positivism is a normative attitude, regulating how we are to use such terms as 'knowledge', 'science', 'cognition', and 'information'" (Kolakowski 1993, 2). Kolakowski (1993, 3-8) characterizes positivism based on three basic assumptions (the fourth he mentioned is quite controversial and interpreted differently within positivism, so one can argue that it is not essential): First, positivism assumes no difference between a touchable, visible surface and a depth-structure of reality that is accessible only by means of theoretical effort; only observable phenomena are real. Second, as a consequence, positivism rejects a correspondence between theoretical concepts and reality; theoretical concepts remain in our heads nominally. Third, positivism is built on a value-free thesis of research. Qualities of things and humans, like "good" or "beautiful" are not part of empirical reality, they are not observable, and lie therefore out of science. Consequently the researcher should not mix up value-leading position with the proper research process.

From that dispute two crucial points, which a critical methodology has to include, but as well to assess, can be identified:

First, how is the relation between the cases which we can study empirically and the macro-level (society) shaped? Here our methodological starting point is the well-known passage from Marx's 18th Brumaire: "Men make their own history, but they do not make it just as they please; they do not make it under circumstances chosen by themselves, but under circumstances directly found, given and transmitted from the past" (Marx 1972, 10). Adorno (1976b, 68) outlines that, in general, social phenomena can be analysed on two different levels: "Some apply to societal totality and its laws of movement, others, in pointed opposition, apply to individual social phenomena which one relates to a concept of society at the cost of obstracization for being speculative. Accordingly, the methods vary". In contrast to that opposition, Adorno calls for a dialectical approach, which assumes society and the individual as mutually conditioned and interrelated. Critical research engages "in the back-and-forth of

studying parts in relation to the whole and the whole in relation to parts" (Kincheloe and McLaren 2005, 312). Such an iterative procedure requires some structure in the research process. If society's quality, as a whole, has some determining influence on the practice of people, then theoretical assumptions about the society should be included in a critical research design to get the iterative or dialectical process of advances in knowledge started. A pure inductionist research can only create an understanding, available to the people studied, but remains silent towards the hidden structures of society (Gorelick 1991, 464). The research process goes back and forth between on the one hand, the deduction of SNS users' arguments about privacy and surveillance from preliminary assumptions about society, and on the other hand our interest in theory creating or reconstruction (Burawoy 1998) based on collected data. Our commitment to the iterative process is both expressed in research structuring questions that are formulated in a qualitative open style and research structuring hypotheses.

Second, what is the role of the researcher within the research process? Adorno states: "Either, knowledge of society is interwoven with the latter, and society enters the science of society in a concrete form, or society is simply a product of subjective reason, beyond all further inquiry about its own objective mediations" (1976a, 2-3). Critical theory and postmodern thinkers have stressed that research always fails to be neutral and the positivist value-free-thesis of research is itself a value. In this context of value-loadeness of research, Max Horkheimer argues that "critical theory has no specific influence on its side, except concern for the abolition of social injustice. This negative formulation, if we wish to express it abstractly, is the materialist content of the idealist concept of reason" (Horkheimer 2002, 242). But how exactly is the researcher's critical involvement in the research process exactly meant? How is Adorno's postulate, that society enters the research in a concrete form, meant? At which stage of the research process Horkheimer's critical criteria of the "good" or the emancipative has an effect? We see two logical possibilities to interpret critical theorists' commitment to emancipation: On the one hand, research is used for emancipation. Results of empirical research, indifferent from what position it comes, are interpreted in terms of critical theory and are situated within societal analysis. Critical research is more about critical interpretation, than critical methods. Or, on the other hand, the research process is itself a part of emancipation. This means stronger methodological consequences in contrast to the dominant research paradigm of positivism. As Fontana and Frey put it for the research interview: "If the interview cannot be a neutral tool (...), why not turn into a walking stick help some people get on their feet" (Fontana and Frey 2005, 695)? People should not be studied as objects, rather than let them participate as subjects in the research process. For instance, feminist methodology demands amongst others that the research process must become a process of conscientization, both for the researched and the researcher (Mies 1993, 72-73) by collectivizing and sharing their experiences of oppression. Such collectivization is a necessary condition of emancipation. But, do we study people who must "get on their feet", as Fontana and Frey say? Are we studying oppressed? In a certain sense

they are and we do. Christian Fuchs (similar Andrejevic 2010) argues that the use of current SNS causes several problems. He refers to "the complexity of the terms of use and privacy policies, digital inequality, lack of democracy, the commercialization of the Internet, the advancement of market concentration, the attempted manipulation of needs, limitation of the freedom to choose, unpaid value creation of users and intransparency" (Fuchs 2011b, 145). So one can conclude that SNS users are oppressed because they are other-directed, manipulated, exploited, and socially sorted insofar as they are reduced to their role as consumers and advertising targets by profit interests.

2. Research questions and hypotheses

After we have made clear what paradigmatic and methodological position our research is coming from, we are now able to substantiate our research interest. The overall research question of our study was:

How are surveillance of data and privacy discussed by SNS users? Which arguments do they use for arguing that they disagree with surveillance on SNS?

In the following section, more specific research questions are derived from our general research interests. Based on our paradigmatic position and existing research, we formulated several hypotheses that lead our attention in order to answer the research questions. Thereby, as surveillance and privacy in the context of SNS have hardly been studied by now, we, on the one hand, partly asked explorative questions and, on the other hand, we had to transfer studies' insights stemming from an offline or an online environment other than SNS, to our new research field.

First we wanted to explore social networking users' notion of surveillance and potential attitudes towards surveillance. The research question (RQ) 1.1 in this context was:

RQ1.1: Which arguments do students use for arguing that they disagree/agree with certain kinds of surveillance on SNS? In the opinion of students who are critical of surveillance on SNS, who or what aspects of life and activities should be protected from surveillance on SNS?

There is no agreement in the literature on how surveillance should be defined. Some see it as a negative concept; others argue that there are also positive qualities of surveillance (Fuchs 2011b). Reasonable criteria of differentiation and valuation are therefore needed. All approaches have in common that they see surveillance connected to the systematic collection, storage, diffusion, processing, and use of personal data. On SNS, student users disclose more personal information than they disclose in general (Christofides, Muise, and Desmarais 2009, 342). Surveillance of users' data can be differentiated according to the entity that conducts surveillance. Who is watching is probably an important aspect of SNS users' assessment of surveillance.

Hypothesis 1a: A typical attitude expressed by SNS users is that they are unconcerned about the use of their data for economic ends because this form of surveillance is mainly invisible and does not show direct visible effects.

Important economic ends of surveillance on SNS are monitoring personal information and profiles by employers in order to improve companies' recruitment; but as well selling content to third parties and targeted/personalized advertising. Most of these opportunities are enabled by the SNS' terms of use and privacy policies (Sandoval 2011). People acknowledge "that they have adopted a laissez-faire attitude to their personal privacy, relying on government and the good will of the organizations with which they do business" (Ekos 2004, 14). Within a surveillance society (Lyon 1994) "the proliferation of technology and instances where personal information or other forms of personal privacy are at stake have become too numerous and complex for the average person to be vigilant about" (Ekos 2004, 14). The vast majority of the Internet users show a "pragmatic" attitude towards privacy issues (Sheehan 2002). Knowledge of surveillance is one important predictor of concern and, in general, knowledge of surveillance techniques is quite low among people (Chan et al. 2008, 9) and social networking users (Fuchs 2010, 177). We hypothesized that knowledge of surveillance, which has to do with the visibility of surveillance and the noticeability of surveillance's effects, are crucial conditions that influence agreement or disagreement with certain forms of surveillance. When it comes to economic surveillance on SNS for targeted advertising purposes, visibility is particularly low as users cannot see how identification, classification, and assessment of their data for targeted advertising purposes works. These processes take place behind the surface of the SNS.

Hypothesis 1b: A typical attitude expressed by SNS users is that they are concerned about job-related disadvantages in their working life caused by surveillance on SNS.

An overall laissez-faire attitude does not exclude concrete concerns. We hypothesized that an important users' line of argumentation to express surveillance concerns is about job-related disadvantages in their working life (Albrechtslund 2008). In comparison to collecting personal data for advertising purposes, with this form of surveillance, a privacy threat and negative personal consequences are more obvious. Therefore we hypothesised that a typical attitude expressed by SNS users is that they are concerned about job-related disadvantages in their working life caused by surveillance on SNS.

Hypothesis 1c: The agreement respectively disagreement with certain kinds of surveillance depends on the extend power is attributed to the particular entity that is watching.

A problematic form of surveillance may therefore be surveillance being based on an asymmetrical power relation between the watcher and the watched, as well as that one resulting in obvious disadvantages for the user (also if the user's disadvantages outweigh eventual advantages of surveillance). Surveillance is overwhelmingly conducted by large organizations, such as states or companies (Gandy 1993, 95; Ogura

2006, 272). States and companies have an interest in control, entitlement, management, influence, or protection; thus they use purposeful, routine, systematic, and focused kinds of watching SNS users. In capitalism surveillance technology "has been designed and is being continually revised to serve the interests of decision makers within the government and the corporate bureaucracies" (Gandy 1993, 95). State or economic surveillance is based on a power inequality between watchers and SNS users (Lyon 2007, 175-176). Power inequality is connected with an unequal distribution of means of surveillance (such as technologies) or an unequal access to them (Fuchs 2011b, 142). Companies like Google or Facebook own great technical means, such as server parks, and human means of surveillance, such as experts (engineers, software developer), but also knowledge, such as elaborate algorithms for searching the web. In general three main directions of surveillance can be identified: First, people watch each other from the same hierarchical level (lateral surveillance) and perceive themselves as equals (Albrechtslund and Dubbeld 2005; Albrechtslund 2008; Dennis 2008; Andrejevic 2005; Mathiesen 1997, 230; 2004, 100). Second, the direction of surveillance – in hierarchical terms - goes from the bottom to the top (bottom-up surveillance; see Mann, Nolan, and Wellman 2003; Haggerty and Ericson 2000; Hier 2003; Koskela 2006). WikiLeaks is an example in this context. Third, top-down surveillance is characterized by people on low levels and without power, watched by power holders on the hierarchy's top (Foucault 1977). We supposed that a sense of hierarchy and power relations is crucial to the users' perception of surveillance and to the likelihood that they argue in favour of surveillance and against privacy. The first two surveillance directions are likely to be welcomed by SNS users. Forms of top-down surveillance are likely to be perceived as problematic privacy intrusion.

Second, we were interested in exploring the concept of privacy that is frequently made use of to oppose surveillance but is as such contested from a critical theory perspective. The corresponding research question was:

RQ1.2: Which role does a reference to privacy play in students' argumentation concerning communication on SNS? What do SNS users mean with "privacy"? What aspects of life should in the opinion of privacy-concerned SNS users remain private on SNS?

Privacy is a current issue in the context of using SNS (Beer 2008, 523-526; Fuchs 2009, 11-22; see also Fuchs 2010, 2011c; Lewis, Kaufman and Christiakis 2008; Lange 2007). Techniques of surveillance enable the vast collection, storage, and assessment of personal data, such as uploaded pictures, chat conversations, clicking behaviour, and profile information about their hobbies, jobs, world views etc. Many authors identify therefore new information and communication technologies in general, and especially the Internet and SNS as a potential privacy threatening environment.

Hypothesis 2a: A reference to privacy is important in the argumentation of privacy-concerned SNS users against surveillance.

Empirical research has confirmed the importance of privacy as a critical domain on the Internet (for example Chan et al. 2008, 20 and in the context of using SNS (boyd and Hargittai 2010; Fogel and Nehmad 2009; Acquisti and Gross 2006; Christofides, Muise, and Desmarais 2009; Debatin et al. 2009; Ellison, Steinfield, and Lampe 2007; Lewis, Kaufman, and Christakis 2008; Livingstone 2008; Dwyer et al. 2010, 2975; Fuchs 2010; Utz and Krämer 2009; Bosau, Fischer, and Koll 2008; Dwyer, Hiltz, and Passerini 2007; Tufekci 2008). Therefore we hypothesized that the reference to privacy is an important line of users' argumentation to express their concerns towards surveillance.

Hypothesis 2b: SNS users typically express a view of privacy that is based on the control theory.

Within the literature of privacy studies, two overall strands of conceptualizing privacy can be identified. The first one is the so called access theory of privacy that sees privacy as the restricted access to a personal realm (Tavani 2008, 142ff; Allen 1988, 3; Bok 1983, 10; Gavinson 1980, 428f). Once the boundaries of this personal realm, the chat room for instance, are crossed, say for instance by statistical analysing tools of the commercial social networking site provider, then users' privacy is violated. Positively put, this means that the restricted access to certain realms is privacy. The other strand is described as control theory of privacy; here privacy is seen as control and self-determination over information about oneself (Tavani 2008, 142ff; Fried 1984, 209; Froomkin 2000, 1464; Miller 1971, 25; Quinn 2006, 214; Shils 1966, 281f; Spinello 2006, 143; Westin 1967, 7). In a control theory not the private character of certain information or realms is crucial but there is privacy even if one chooses to disclose all personal information about oneself. Otherwise in an absolute restricted access theory of privacy, there is only privacy if one lives in solitary confinement without contacts to others; hence the restricted access theory links privacy to secrecy. For instance, a control theory of privacy may in contrast stress that the use of sensitive personal data for targeted advertising is not necessarily a privacy violation if opportunities for individual decisions (such as opt-in advertising settings) exist that allow users to individually choose which data they want to make available for targeted advertising and which one not. On the other hand, an access theory of privacy may stress that there is certain personal data (such as sensitive information about political views, sexuality, health status, intimate relations, membership in associations and trade unions, communication contents, etc) that should in principle not be used for advertising e.g. and that an access of targeted advertising to such data is always a violation of privacy.

Hypothesis 2c: SNS users typically express a view of privacy as an extrinsic value

Tavani (2008) points out that privacy can be seen as a unitary concept that stands on its own, as derivative concept that is derived from other concepts such as property, freedom, and autonomy, or as multifaceted notion. James Moor (1997) speaks in this context of intrinsic and instrumental ways for justifying privacy. Mindful of the

modern privacy debate's starting point (Warren and Brandeis 1890), one could argue that the right to privacy has always been linked with the liberal core value of the individual's negative freedom from public and society (Rössler 2001, 20-21). To stress that linkage between privacy and liberalism means not that the concept of privacy covers no intrinsic aspects of human life. On the contrary it indicates that people see privacy not as standing on its own; rather they may refer to other ends and values, such as those propagated in the liberal tradition of thinking, namely property, individual freedom, and individual autonomy. In accordance with many privacy scholars (Fried 1984; Rachels 1975; Reiman 1976; Altman 1976; Gavinson 1984; Rössler 2001; Bennett and Raab 2006; Warren and Brandeis 1890; Westin 1967), we hypothesized that SNS users typically express a view of privacy as an extrinsic value.

Hypothesis 2d: SNS users see privacy as private property.

According to our research framework we think that there is a close link between private property and privacy. Today "the package of rights called 'property' includes: claim rights to possess, use and receive income; powers to transfer, waive and exclude; a disability (a no-power) of others to force a sale; liberty rights to consume or destroy; and immunity from expropriation by the government" (Munzer 2005, 858) and others. In capitalism having private property is essential as it became the most powerful mean to self-development. We interpret that privacy as private property is an influential concept.

Third, as our critical political economy approach suggests, we were especially interested in exploring economic forms of surveillance. Targeted advertising on SNS can be interpreted as economic surveillance because it requires a lot of personal user data to perform. So we were interested in SNS users' attitude towards targeted advertising and also potential funding alternatives:

RQ1.3: How do SNS users think about targeted advertising and alternative funding models? How do they relate this topic to privacy and surveillance issues?

Targeted advertising is only one form of several funding models of SNS that one can imagine. We are therefore interested in exploring how people value privacy and surveillance issues in the context of alternative funding models. As an alternative, non-commercial funding of SNS, a public funding (as applied to the radio and television media sector in Austria) or a donation model (like Wikipedia), for instance, are imaginable.

Hypothesis 3b: SNS users say that public funding of SNS is a better option than advertising-financing. Those who express doubts argue that public funding or alternative funding strategies (like donation models) tend to be inefficient and ineffective.

It is likely that users have assumptions about the effectiveness and efficiency regarding potential funding models that influence their assessment of privacy and surveillance on SNS. Those who desire targeted advertising because it supports individual consumption, those who think that an advertising funding serves them money, and

those who have general concerns towards non-market financing, probably would not vote for an alternative, non-advertising funding of SNS. All users who hold those positions are likely to describe alternative funding models to be inefficient and ineffective. Those SNS users who perceive targeted advertising as annoying, as well as those (see hypothesis 3a) who see the linkage between the commercial character of SNS, intensified surveillance measures, and a privacy threat, would probably prefer an alternative funding model.

Hypothesis 3a: SNS users typically argue that they do not see targeted advertising as a privacy threat and not as a problematic form of surveillance.

First, surveys found that users' knowledge about privacy issues on SNS is very low (Acquisti and Gross 2006, 51-53; Ellison, Steinfield, and Lampe 2007) or they have skewed sense of what privacy settings exactly entail (Debatin et al. 2009, 100). This lack of knowledge can also be applied to the linkage of targeted advertising and privacy (settings) (Turow et al. 2009, 3). Exceptional cases might however occur if the business model and privacy settings of SNS have recently changed and these changes are accompanied by public discussions in the traditional media and online discussion groups (Fuchs 2010, 181), or, on the individual level, if users had heard of a privacy invasion happened to others (Debatin et al. 2009, 100). Second, a lot of (commissioned) research was conducted in order to clarify companies' opportunities to increase customers' perceived control of information within business models that depend on consumer surveillance. For example, a highly cited survey by Culnan and Armstrong (1999) found that fair information procedures that bring about an increased control over personal information decrease privacy concerns of consumers. Most of these surveys try to find out how one can build up trust between customers and companies and how to establish fair interactions between them. Exactly therein lies the commissioner's commercial interest (Gandy 2003, 294-296). As a result, one could argue that the intense research and practical effort that has been initiated by commercial interests has decreased users' perception of targeted advertising as a privacy threat. Users may feel being in control and threaten fairly. Insight into the use of personal through SNS providers is due to complicated terms of use and privacy statements hardly given. Companies' courses of business are normally kept secret and this secrecy/privacy is guaranteed by law as well as by the right to private property in capitalism. Therefore using SNS is largely based on an "uninformed consent" (Campell and Carlson 2002, 593). Less visibility of surveillance for targeted advertising plus less visibility of its effects for the users let us hypothesise that users tend to see targeted advertising not as a privacy invasion or problematic form of surveillance.

Apart from surveillance and privacy threats, SNS are popular because they obviously offer user benefits. We were interested in exploring how privacy-user benefits trade-offs work and what role surveillance plays within users' considerations. In this context we asked:

RQ1.4: Do students think that there is a privacy-user benefit trade-off on SNS? Why respectively why not? In this context, which arguments do they employ to argue for privacy and against surveillance on SNS? Which arguments do they employ to argue for surveillance and against privacy on SNS?

Livingstone (2008, 406) found in her empirical study among teenagers that privacy intrusions are that aspect of online social networking which users want to change mostly. However, as for example a study by Debatin et al. showed, the benefits of SNS can "outweigh privacy concerns, even when concrete privacy invasion was experienced" (Debatin et al. 2009, 100). For example, a frequently identified privacy paradox discussed is the gap between individuals' intentions to disclose private issues and individual's actual disclosure behaviours (Norberg, Horne, and Horne 2007; Barnes 2006). Benefits that make people to give up their privacy and to accept surveillance, need to be understood in a broad sense. A benefit can be a financial or economic offer as well as a social advantage. In capitalism, people often can achieve advantages exactly through accepting disadvantages; they are compelled to manage conflicting consciousness (Turow and Hennessy 2007, 309). It is likely that users name benefits, which are related to social capital, such as maintaining friendships and communicating (Lenhart and Madden 2007; Ellison, Steinfield, and Lampe 2007; Fuchs 2010; Zywica and Danowski 2008). From the users' point of view these benefits are obviously worthy to take a, at least partial, loss of privacy. An example is accepting disruptive targeting advertising in order to benefit from the social networking site's communication opportunities.

RQ1.1. is the most comprehensive of our research questions, RQ1.2, 1.3., 1.4 can be deduced logically from it. Privacy, and therefore RQ1.2 and 1.4, is a common argument made to disagree with surveillance. To explore the meaning of privacy is at the same time answering the question, who or what aspects of life and activities should be protected from surveillance on SNS. A certain kind of surveillance, which was of particular interest in our study, is economic surveillance performed structurally by the SNS provider due to advertising purposes. According to our methodological approach we have an interest in critique of existing social relations in general, surveillance and its economic reasons in particular. Alternative SNS that are not funded by the surveillance/targeted advertising model become relevant for us. Consequently RQ1.3 can also be deduced from RQ1.1.

3. Study design

The literature of privacy and surveillance studies shows that little qualitative research has been conducted, especially concerning social media and SNS. The kind of study that we conducted in order to explore our research questions and hypotheses is best described as an explanatory and instrumental case study (Babbie 2010, 94; Punch 2005, 144). Our study was qualitative, however, in accordance with our methodology, broadly structured. That means that the study rather looked for answers

than questions because it was based strongly on theoretical considerations that have been developed before.

It is crucial to have in mind that theory verification can also be done by qualitative research. We hoped that our empirical results can, in a wider context, contribute to a reconstruction (Burrawoy 1998, 16) of critical political economy theory of surveillance and privacy. By the means of qualitative interviews, we expected a holistic picture about certain privacy and surveillance issues that are applied by SNS users, and as well a picture from the inside of these actors' perception. For example, we expected to explicate the ways how people manage the contradiction between privacy and surveillance within their day-to-day usage of SNS. Political economy of privacy and its link to corporate surveillance has hardly been studied. The category "privacy" has been used within researches in a non-reflective manner, based on classical liberal mainstream theory. We were interested in the link between, on the one hand, privacy, private property, competitiveness, and, on the other hand, economic surveillance.

What we can learn from already conducted qualitative research is that people do not think about privacy and surveillance on a day-to-day basis (Ekos 2004, 15); therefore it is crucial to design research instruments in a way that reflects everyday contexts and experiences of the studied individuals (see for example Nowak and Phelps 1992, Wang and Petrison 1993). Privacy is a complex issue and its meaning depends strongly on the context, within which it occurs. Additionally, it is not obvious that targeted advertising is a form of surveillance. We supposed that the underlying economic dimension of privacy and surveillance is quite unknown among SNS users (see above). Our context was mainly data privacy on SNS. Within that context, economic surveillance and its individual and social disadvantages as well as potential alternatives to it, lie at the bottom of our critical theoretical effort. Therefore, providing privacy and surveillance scenarios that are likely to occur or had already occurred in the everyday reality of the SNS users seemed to be useful. For this purpose, the social research literature suggests applying the vignettes approach (Finch 1987; Barter and Renold 1999; Foddy 1993, 50). Finch describes vignettes as "short stories about hypothetical characters in specified circumstances, to whose situation the interviewee is invited to respond" (1987, 105). In qualitative research, "vignettes enable participants to define the situation in their own terms" (Barter and Renold 1999). We developed such scenarios or contexts from information that is given within the SNS providers' terms of use and privacy policies (see interview guide).

As we analysed SNS users as exploited, we could also follow a more empathic approach within the interviews (section 1). That meant to switch between the two outlined methodological positions of critical research according values (research should be interpreted critically or research is intrinsic critical). Our commitment to emancipation has shaped the method of data collection. In this context, critique of ideologies demanded a more objective position of the researcher towards the researched. On the other hand emancipative research interests demanded identification with the researched; this meant, similar to Gilliom's study in the context of the welfare system (2001, 151-152) to inform the interviewees about the social and individual disad-

vantages of economic surveillance by providing them corresponding information and potential alternatives. We therefore used a two-part interview structure: Initially, we asked interviewees questions about their knowledge and opinions regarding all our research questions. Then, additionally in respect of research question 1.3, we provided them with some information about how economic surveillance works on SNS and about potential alternatives to it (see interview guide). Based on this information, we expected a kind of learning effect among the interviewee within the interview.

Our qualitative research aimed at conceptualizing privacy and surveillance and new hypotheses about these issues in the context of a theoretical framework; it was explanatory in that sense. Our research interest was directed from the abstract of theory, to the concrete of in-depth case study, to again the abstract of improved and more detailed theory. As qualitative methodologists (Punch 2005, 146-147; Miles and Huberman 1994, 36; Kvale 2007, 124; Ward Schofield 1993, 221) stress, the theory-directed design of our research, which seeks to abstract and conceptualize concrete observations, contributes to external validity/generalizability of the research. In the following subsections (3.1 to 3.3) important aspects of our study design, namely the sampling, data collection, and data analysis, are described. These steps were also evaluated according scientific quality criteria. Thereby we agree with Punch (2005) who stresses the research question-method-fit as the central criterion of internal validity.

3.1. Sampling

We studied the social unit of Austrian students, who have had collected experience in using SNS at the time of 2011/12 when our study takes place. The use of SNS is very common among students; some of the best-known social networking platforms have been arisen from a student context (for example Facebook and studiVZ). To select a sample, we applied a form of purposive or conceptually driven sampling, which can evolve during the fieldwork (Miles and Huberman 1994, 27) and seeks to "maximise theoretical development" (Arber 1993, 74) in accordance with our structured approach. Our sample included similar and different cases. We asked a group of interviewees who is especially critical of (economic) surveillance and has a high knowledge about privacy issues, as well as a group of less concerned (standard) users. We were interested in studying "what is" (Ward Schofield 1993, 209), as well as "what could be" (Ward Schofield 1993, 216-219).

Our sample eventually consisted of 30 Austrian students who used or are using SNS in the age between 20 and 34 (mean = 24,9 years, standard deviation = 3,33 years), found in the area of Salzburg, Austria. The gender distribution among the participants was two-thirds women, and one-third men. Participants came from a broad range of academic disciplines and studied at one of the universities in Salzburg; the focus was natural sciences, including engineering and informatics on the one hand, and on the other hand humanities and social sciences. 3 out of 30 came from law or economic sciences (which is offered combined at University of Salzburg).

Studying "what is" calls for sampling the typical social networking user. This increased the external validity, respectively the generalizability of our qualitative research. Thereby studying the typical is not studying the randomly selected; rather it is a theoretical effort to anticipate the typical. We expected that the typical SNS user occupies oneself not with studying SNS or is not politically engaged in data protection. To sample the typical we paid attention for a balanced distribution among gender, age, study subject and socioeconomic status. We selected missing types of students on behalf of a small questionnaire polling socio-demographic data (age, study field, duration of study, and social status) that was provided to the interviewee.

Studying "what could be" was one of our research goals which are based on a critical and emancipative approach. Studying "what could be" "refers to locating situations that we know or expect to be ideal or exceptional on some a priori basis and studying them to see what is actually going on there" (Ward Schofield 1993, 221). On the one hand, we thought that studying experiences with alternative SNS, such as Diaspora and kaioo, could be useful and should be considered in the process of sampling. Therefore we searched through the alternative networks in order to detect potential study participants from the area of Salzburg. As alternative SNS are not broadly known and used, it was hard to find people experienced in using these alternatives. However, tracking back a little campaign to advertise Diaspora launched online by a Salzburg student party, we ultimately ensured to include experiences with alternative SNS in our sample. We expected interviewees, who are experienced in using alternative SNS, such as Diaspora as overall critical of commercial SNS. On the other hand, during the time we were planning our study, some discussions about online privacy emerged because of the introduction of a mandatory mail system for students at the University of Salzburg. That mail system is operated by Google. Many members of the university expressed their privacy concerns towards this external and commercial player. We assumed that participants in these discussions are likely to be non-standard user of SNS, maybe that they are more critical, privacy sensitive and aware of surveillance. Therefore they represented an important contribution to our sample. We attended the pertinent discussion and online groups and succeed in finding interviewee there. A further dimension of critique in which we were interested is to sample student who are critical towards advertisement (on SNS). To be critical towards privacy issues and to be critical towards economic issues do not coincide automatically. To sample the latter dimension of critique, we assumed that views from the social science, cultural science, and humanities contrast with views from the management, business, and law sciences. Both perspectives were included within our sample and indeed we could observe that law, business, and economic students in our sample agree with advertising in general and on SNS; whereas the distribution in attitudes towards this issue was more balanced among interviewees from other study fields. We also included interviewees who are known as political activists being critical of surveillance as well as economic issues into our sample. Additionally we assumed that interviewees who have quit using SNS can contribute to our research interests by understanding their reason to behave so.

The first contact with the interviewees was established by providing them short information, that included by whom the study is conducted, a neutral expression of our purpose, the importance of being part of it (works as a symbolic incentive for the potential interviewees), a commitment to confidential and anonymised publication, the estimated duration of the interview, and the request for an appointment.

After a couple of interviews (20), it became increasingly difficult to find further interviewee by the hitherto followed snow ball principle of asking "friends of friends" or candidates who were suggested by interviewees. Therefore we decided to announce our study publicly on behalf of the student union's email newsletter. We used the same first contact information but in order to ensure positive feedback we rewarded participants with 20 Euro Amazon vouchers. The so found interviewees completed our sample as they participated due to other incentives than doing a favour.

Table 1 lists age, gender, study field, and purpose to include it into our sample for each interviewee.

Interviewee Number	Age in years	Gender	Field of study	Semester studied	Purpose to include the person into the sample
1	30	male	Natural science	10	participation in events about data protection; expected to be privacy sensitive
2	23	male	Natural science	2	has quit using SNS, expected to be critical of SNS in general
3	23	female	Humanities and cultural science	6	participation in events about data protection; expected to be privacy sensitive
4	24	female	Law and economics	8	Expected not to be uncritical of advertising, expected to have knowledge about privacy
5	25	female	Natural science	8	Expected to represent the typical
6	25	male	Social science	12	participation in events about data protection; expected to be privacy sensitive
7	27	male	Informatics and computer science	2	Known for using alternative SNS, expected to be privacy sensitive
8	23	female	Humanities and cultural science	6	Expected to represent the typical
9	22	female	arts	6	Supplement to the range of included study fields; has quit using SNS, expected to be critical of SNS in general
10	34	female	Humanities and cultural science	6	Expected to represent the typical
11	24	male	Social science	8	Expected to represent the typical
12	21	female	theology	4	Supplement to the range of included study fields; expected to represent the typical
13	23	female	medicine	6	Supplement to the range of included study fields; expected to represent the typical
14	21	female	Technical and engineering science	6	Supplement to the range of included study fields; expected to represent the typical
15	23	female	medicine	8	Supplement to the range of included study fields; expected to represent the typical
16	30	male	Informatics and computer science	16	Member of the student party propagated alternative SNS; expected to be experienced in using alternative SNS, political activist who showed critical attitude towards surveillance and advertising
17	26	male	Social science	11	Expected to represent the typical
18	23	female	Social science and natural science	5	Member of a student party propagated alternative SNS; expected to be critical of surveillance and advertising
19	30	male	Social science	3	Member of the student party propagated alternative SNS; participation in events about data protection; expected to be experienced in using alternative SNS, critical attitude towards surveillance and advertising
20	25	female	Natural science	8	Expected to represent the typical
21	24	female	Natural science	8	Expected to represent the typical
22	24	female	Social science	8	Other incentive than doing a favour; expected to represent the typical
23	25	female	sports	11	Other incentive than doing a favour; expected to represent the typical
24	20	female	Humanities and cultural science	2	Other incentive than doing a favour; expected to represent the typical
25	24	female	Natural science	11	Other incentive than doing a favour; expected to represent the typical
26	22	female	Natural science	8	Other incentive than doing a favour; expected to represent the typical
27	24	female	Humanities and cultural science	11	Other incentive than doing a favour; expected to represent the typical
28	32	female	Law and economics	20	Expected not to be critical of advertising, expected to have knowledge about privacy
29	28	male	Social science	3	Other incentive than doing a favour; expected to represent the typical
30	24	male	Humanities and cultural science	2	Political activist who showed critical attitude towards surveillance and advertising

Table 1: Overview of the sample

3.2. Data collection procedures

According to our theoretical work (section 1 and 2) we conducted qualitative interviews that should not be completely unstructured; therefore we applied semi-

structured interviews and used an elaborate interview guide. Our study represents a single point in time (Babbie 2010, 106). All interviews were audio-taped. In the interviews we applied questions for interviewees' attributes, attitudes, and beliefs according to what is about surveillance and privacy, how something works in that context, and why they think so (Newell 1993, 95).

On the one hand, some structure within the interviews contributed to comparability between the single interviews and between our results and the study's survey data. Some structure was further appropriate for theory-testing and our explanatory intent (Miles and Huberman 1994, 36). We considered that rich context description of each interview setting is important to a lesser extent. Therefore we noticed no more information than where and when the interview happened, and if any unexpected situation arose. Nevertheless our purposive sampling strategy was described in each case. On the other hand, Nigel Fielding outlines some criteria when to apply non-standardised interviews. Such method is useful "to get acquainted with the phraseology and concepts used by a population of respondents" (N. Fielding 1993, 137) and "the non-standardised approach is also valuable where the subject matter is sensitive or complicated" (N. Fielding 1993, 138). Both criteria fit to our research interests, as should be readily apparent from the previous discussion (studying "what is", privacy and surveillance are sensitive issues and complicated concepts) and indicated the semi-structured approach ultimately.

Our method has the additional advantage to "bring out the value-laden implications of response" (Merton cited in N. Fielding 1993, 148). Therefore it was important that the interviewer shows an attitude of openness and that he encouraged interviewees to communicate their feelings and fears during the interview. A few pilot interviews helped us to achieve high reliability and less reactivity standards of our research and to develop an interview guide. The fact that the interviewer is part of the studied population may minimize interviewer effects (N. Fielding 1993, 145; otherwise Foody 1993, 125). Traditional reliability standards cannot be transferred easily from the quantitative approach to qualitative interview situations (Kvale 2007, 122). In our case reliability is a matter of interviewer's craftsmanship and of detailed publishing the interview guide and our sample strategies. A basic problem of interview research is the "correspondence between verbal responses and behaviour, the relationship between what people say, what they do and what they say they do, and the assumption that language is a good indicator of thought and action" (Punch 2005, 176). We hoped to minimize that basic problem insofar as we were not mainly interested in respondents' behaviour, but in their lines of argumentations and justifications.

3.2.1. Interview setting

The interviews took place in an environment that was familiar to the interviewee, namely a room at the university or their own home. Duration of the interviews was between 60 and 135 minutes. The most interviews lasted on average about 100 minutes.

In the beginning, interviewees were informed of how we will use the collected interview material and were asked to sign a consent letter and for their permission to record the interview. Further, they were provided with basic information about our research project on behalf of a handout that entails basic and contact information. We used an interview protocol sheet to note the interview date and location, their incentive to participate, any particular events in contacting or during the interview, rudimentary information about the interview atmosphere, and potential abnormalities within the interview interaction. The interview started then with simple and easy questions in order to get the interviewee engaged with our topic and ended with open questions about whether interviewee want to add something. To introduce the more emphatic part of the interview, a handout was provided and went through with the interviewee. The handout contained a short definition of the targeted advertisement funding model of SNS and lists in detail which personal information FB can use for that purpose. After the interview was finished, the interviewees were asked for filling the small socio-demographic questionnaire (Newell 1993, 108) and if they wish to receive the transcript and/ or information about related publications by the research project.

3.2.2. Interview guide

The applied instrument was an interview guide that includes research areas with respective proposal questions as well as proposals for probing questions (potential rephrases of questions). Probing questions or follow-up questions were used for receiving a richer response. In the first instance they should encourage the interviewee to explain the main questions further (expectant glance or silence, asking “what else?” or “can you tell me more?”). In the second instance they referred to our hypotheses (if they are not yet touched). A given order of research questions was not mandatory; however the research question 1.3 always stood at the end of the interview (see above).

The provided information during the interviews included, first, stetting our topic in a very neutral way because interviewees tend to give those answers they anticipate the interviewer wants to hear: “If researchers fail to indicate how they define their research situations, respondents will search for clues (and even make guesses about the researchers’ definitions of the situations), to help them interpret the researchers’ acts” (Foddy 1993, 21). Then consequently, each of the respondents will answer a different question. Second, information/ scenarios about privacy and surveillance were given unitarily because they should clarify our context in the same manner across the interviews. Third, information about economic surveillance was provided in an educational way in order to introduce the more emphatic interview part. Within that concluding part of our interviews a personalization, by referring back to personal experiences with economic surveillance on SNS for instance, often was an opportunity to gain in depth insights (N. Fielding 1993, 139). Here sometimes leading questions were more useful to “evoke a deeper and more thoughtful response than a bland

question which receives only a conventional and unreflecting answer" (Newell 1993, 105).

On 07.09.2011, during our data collection phase, FB changed its privacy policy. These changes affected the appearance/ layout of the policy, but also some of its content and therefore also our interview guide. In terms of layout the policy extended in length, but became more categorized. In terms of content some new elements were included; however these changes didn't affect our interview guide substantially as economic surveillance were still needed to finance FB. In order to ensure that interviewee understand what we are asking for, those passages of the interview guide that refer literally to FB's privacy policy were adapted. According to the new scheme of categorisation within FB's privacy policy, the part of the interview guide, which was at the same time the handout about the information collected by Facebook for advertising purposes was also adopted. To comprehend the instrument and its changes in detail, please see table 2. In the left column questions used before FB changed its privacy policy are listed, in the right column questions used after FB changed its privacy policy are listed.

FINAL VERSION OF THE INTERVIEW GUIDE

(If changes were necessary due to FB's changed privacy policy, the former passages, in the left colum, were contrasted by the new passages, in the right column)

ICEBREAKER:

IQ1. Have you any questions concerning our study or about the interview procedure?

IQ2. At the beginning, I'm interested in which SNS you know and which you make use of? Since when? How often?

In our study we are particularly interested in what students think about issues of surveillance and privacy not only in the context of SNS, but also in general.

The term "surveillance" is multi-faceted and different people mean different things when talking about surveillance.

IQ3. What comes into your mind, when you are thinking of surveillance? In general, what does it mean to you? *(relates to RQ 1.1, H 2a)*

PROBING: Are you linking certain issues, situations or other themes to the term "surveillance"?

IQ4. Who could watch/ surveil you at using SNS? To what end? *(relates to RQ 1.1)*

PROBING: What about companies? Which reasons they may have?

IQ5. Do you think it is OK that companies watch/ surveil you while using SNS? In which cases? In which not? *(relates to H 1a, H 2a)*

PROBING: Do you bother when your employer or your potential employer follows your activities on SNS? Has this ever happened to you? Do you know such cases and can you tell me about them? What do you think about them? *(relates to H 1b, H 2a)*

If privacy was brought up before: In arguing against surveillance, you have mentioned the term "privacy" …

If privacy wasn't brought up before: Some people mention that they want to see their privacy protected, when they argue against surveillance…

IQ6. What do you understand by privacy? *(relates to RQ 1.2, H 2b, H 2c, H2d)*

PROBING: I know that is a very abstract question, but take your time and try an answer?

IQ7. Can you describe a situation, taken from your real life, within which privacy is or was important to you? *(relates to RQ 1.2, H 2b, H 2c, H2d)*

It could be a situation, within which you missed privacy or in which you were glad to have privacy.

PROBING: Please, think about why privacy was or is important to you in this situation and tell me the reasons?

IQ8. Are there limits of privacy for you? Which affairs or information do you think shouldn't be private at all? *(relates to RQ 1.2, H 2b)*

IQ9. I am giving you now two statements; can you tell me which one is more appealing to you? *(relates to RQ 1.2, H 2b, H 2c, H2d)*

Statement 1: Everyone should decide oneself upon which information should be private and which information he/she wants to publish on SNS. Statement 2: There is information that should be always and mandatory for all private and never be public.

PROBING: Why is this more appealing to you?

PROBING IF STATEMENT 2 WAS CHOOSEN: Which information has you in mind? Should there be any laws regulating which data a SNS user can publish and which should remain private? Why resp. why not?

I'm now interested in your thoughts about the following situation that can arise when using Facebook (see point four of FB's privacy policy): You permit a trusted friend to see detailed profile information, for example your political attitude. Your friend uses an application that surveys FB users' attitude towards important issues within the Austrian election campaign. This application requests also data about you, that only your friends can normally see, for example your political attitude and your friend permit the application to access your data indirectly.

I'm now interested in your thoughts about the following situation that can arise when using Facebook (see point 3.3. of FB's privacy policy from 07.09.2011): You permit a trusted friend to see detailed profile information, for example your political attitude. Your friend uses an application that surveys FB users' attitude towards important issues within the Austrian election campaign. This application requests also data about you, that only your friends can normally see, for example your political attitude and your friend permit the application to access your data indirectly. (INFORMATION: Data, which can be shared by friends, can be regulated within the privacy settings; excluded are those data that are set "public" and standard date like friends list, gender etc.)

IQ10. What do you think about this situation? Would you say that it is an invasion of your privacy? Why? *(relates to RQ 1.2, H 2b)*

PROBING: Would it make a difference if you were informed about the application's access? Would it make a difference if you were also asked for permission?

IQ11. While using SNS, have you ever felt threatened in your privacy? *(relates to RQ 1.2, H 2b, H 2c, H2d)*

PROBING:

If yes, can you tell me about? If no, can you imagine if this would be the case?

What exactly was the threatening?

Please, imagine a situation within the university. Think about a situation in class, there are you, your colleagues, and a professor.

IQ13. What do you think of colleagues using SNS to learn more about you or other students or using SNS to catch up on tests or lecture notes? Are you familiar with that? *(relates to RQ 1.1, H 1c)*

PROBING: Would you refer to that as surveillance or privacy intrusion? Why?

IQ14. Do you think that professors also have FB profiles? What do you mean, is it interesting to have a look on such profiles? Why? *(relates to RQ 1.1, H 1c)*

PROBING: Would you refer to that as surveillance or privacy intrusion? Why?

IQ15. What do you feel about professors observing you or other students on SNS? Do you think that happens? *(relates to RQ 1.1, H 1c)*

PROBING: Would you refer to that as surveillance or privacy intrusion? Why?

I will now describe you a scenario that can arise when you are using SNS: The scenario is about Martina. By now she was not at FB, however she has heard from a friend that FB is useful to find and get in contact with former school colleagues. Therefore Martina decides to create an FB account. At registration, she is informed that creating an account means also to accept the FB's terms of use and privacy policy. There were provided links to these documents and Marina noticed that these documents include several pages small-written text. Right at the start of the terms of use, Martina reads that all posted information still belongs to her (see terms of use from 25.03.2011, point 2). Additionally she reads that FB values the privacy of its users and gives further information within its privacy policy. At the beginning of the privacy policy FB states that it worries about the users' privacy and subjects to data protection regulation and EU directives (see privacy policy from 22.12.2010, point 1). For now, Martina is confident and joins FB because she wants to contact her former school colleagues.

I will now describe you a scenario that can arise when you are using SNS: The scenario is about Martina. By now she was not at FB, however she has heard from a friend that FB is useful to find and get in contact with former school colleagues. Therefore Martina decides to create an FB account. At registration, she is informed that creating an account means also to accept the FB's terms of use and privacy policy. There were provided links to these documents and Marina noticed that these documents include several pages small-written text. Right at the start of the terms of use, Martina reads that all posted information still belongs to her (see terms of use from 25.03.2011, point 2). Additionally she reads that FB values the privacy of its users and gives further information within its privacy policy. At the beginning of the privacy policy FB states that it worries about the users' privacy and subjects itself to data protection regulation and EU directives (see privacy policy from 07.09.2001, point 6.1). For now, Martina is confident and joins FB because she wants to contact her former school colleagues.

IQ16. For which reasons are you using SNS? *(relates to RQ 1.4)*

PROBING: What means … for you?

IQ17. Have you read the terms of use and privacy policies of FB or other SNS? Why? *(relates to RQ 1.4, H 1a)*

FB changes its terms of use and privacy policy many a times. The last time in December 2010 and March this year (2011). When they are changing and you are further using FB, you agree with the changes automatically (see terms of use from 25.03.2012, first sentence and point 13).

FB changes his terms of use and privacy policy many a times. The last time in March this year (2011) (terms of use) and very recently its privacy policy in September this year. When they are changing and you are further using FB, you agree with the changes automatically (see terms of use from 25.03.2012, first

sentence and point 13).

IQ18. Have you realized such changes? *(relates to RQ 1.4, H 1a)*

PROBING: Have you been informed about these changes by media coverage or other users' postings?

IQ19. Concerning data protection, what do you feel when such changes happen? What do you think, why such changes are made? *(relates to RQ 1.4)*

IQ20. Are you happy with FB's existing terms of use and privacy policy? *(relates to RQ 1.4)*

PROBING: Is there anything, which you would add to or except from the terms of use and privacy policy?

Within the scenario, Martina was aware that she agrees with the FB's terms of use and privacy policy. She wanted to find and contact former school colleagues, therefore she agreed.

IQ21. How was that at yours? Are you worrying about your privacy, when you agree to the terms of use and the privacy policy? *(relates to RQ 1.4)*

PROBING: How are you estimating privacy issues in comparison with your reasons to use SNS?

In the last part of the interview I want to talk about the funding of SNS with you. I'm here interested in your opinions.

IQ22. Do you know how SNS get financed? *(relates to RQ 1.3, H 3a, RQ 1.1, H 1a)*

IQ23. What do you think about advertisements on SNS? What do you know about that issue? *(relates to RQ 1.3, H 3a, RQ 1.1, H 1a)*

PROBING: Are you offered useful information from advertisements on SNS? Why?

IQ24. Do you think that advertisements and in a broader sense marketing activity determine the appearance and the functions of FB in a way? *(relates to RQ 1.3, H 3a, RQ 1.1, H 1a)*

IQ25. Have you informed yourself about the use of your data for advertising purposes? *(relates to RQ 1.3, H 3a, RQ 1.1, H 1a)*

PROBING: Have you looked up in the terms of use or the privacy policy for this issue? Have you been informed about this issue by media coverage or other users' postings?

IQ 26. What do you know about the use of your data for advertising purposes? Can you tell me an example how your data is used for this purpose? *(relates to RQ 1.3, H 3a, RQ 1.1, H 1a)*

Let us come back again to the Martina-scenario. Martina has actually met her former school colleagues on FB; she has chosen her privacy settings and then she takes some time to reread the terms of use and privacy policy closer. Within the privacy policy, she found as passage that says: "We allow advertisers to choose the characteristics of users who will see their advertisements and we may use any of the non-personally identifiable attributes we have collected (including information you may have decided not to show to other users, such as your birth year or other sensitive personal information or preferences) to select the appropriate audience for those advertisements. For example, we might use your interest in soccer to show you ads for soccer equipment, but we do not tell the soccer equipment company who you are" (see privacy policy from 22.12.2010, point 1). Obviously the usage of data for advertising purposes doesn't fall within the protection of privacy for FB.

Let us come back again to the Martina-scenario. Martina has actually met her former school colleagues on FB; she has chosen her privacy settings and then she takes some time to reread the terms of use and privacy policy closer. Within the privacy policy, she found a passage which says that Facebook is allowed to use non personalized data for advertising purpose (see privacy policy from 07.09.2011, point 1.4 und 4.1). Such data can be used even you decided not to share them with others. For example, your interest in soccer can be used to show you ads for soccer equipment, but the soccer equipment company is not told who you are. Obviously the usage of data for advertising purposes doesn't fall within the protection of privacy for FB.

IQ27. How do you feel about that FB can use your data also independently from your privacy settings? *(relates to RQ 1.3, H 3a)*

At this point of the interview I want to share some information with you about how advertising funding on FB works. For this purpose, I brought a handout and want to get through it with you.

HANDOUT IS PROVIDED

So called tailored or targeted advertising is the most common form of funding SNS. It presupposes detailed knowledge of users' (consumer) habits, preferences, and needs. Such knowledge enables to make adverts much more accessible to consumers and to trigger purchasing eventually. Therefore, information about users are systematically collected, stored, and evaluated on SNS. Some of the information has to be posted by the user, but there is also a lot of information, which is created during the actual usage of SNS. If one bothers to read the terms of use and privacy policy of FB, one can learn that the following information is collected by FB:

- *Your name*
- *Your profile picture*
- *Your gender*
- *Your "networks", for example of your university or your employer*
- *Your friend list*
- *Your job and your education*
- *Your residence and your home*
- *If you access FB via a computer, mobile phone, or other devices, FB collects information about the kind of access*
- *Your type of internet browser*
- *Your current location*
- *Your IP-address*
- *Information about all your visited web pages while*
- *Registration information, like your name, email-address, birthday, gender*
- *Your profile picture, profile picture, networks, username, and User ID*
- *Information you have chosen to share: when you post a status update, upload a photo or comment on a friend's post. It also includes the information you choose to share when you*
- *Facebook collects metadata of your activities, such as the time, date and place you took the photo or video; your IP address, location, the type of browser, and your system software.*
- *Facebook also collects information about other web pages you visit.*
- *Facebook uses information about your activities on oth-*

town • *Your likes, interests, activities, and connections* • *Your postings, such as pictures, status messages* • *Information about your family and your relationship status* • *Your biography and favourite citations* • *Your web address* • *Your whereabouts* • *If you add connections* • *If you join a group* • *If you add a friend* • *If you create a photo album* • *If you send a gift* • *If you "poke" another user* • *If you "like" something* • *If you attend an event* • *If you authorize an application* • *If you share a video with others*	*logged in (see privacy policy from 22.12.2010, point 2)* • *FB collects information about you on behalf of other users. For example, when a friend tags you on a photo, in a video, or at a location; or when a friend gives details about your friendship or point to a relationship with you. (see privacy policy from 22.12.2010, point 2, last paragraph)* • *FB also collects information about your user behaviour on other websites that are related to or cooperate with FB (see privacy policy from 22.12.2010, point 2)* • *FB, in turn, allows a wide range of advertising networks to track your activities on the site in order to evaluate the adverts. To that end advertising networks store small files, so called "cookies" on your device. (see privacy policy from 22.12.2010, point 4, next to the last paragraph)*	*take an action, such as when you add a friend, like a Page or a website, tag a place in your post, find friends using our contact importers or indicate you are in a relationship.* • *Facebook also collects information others share about you: such as when a friend tags you in a photo or at a location, add you to a group, or provides details about your relationship status.* • *Facebook collects information about you from the games, applications and websites you use friend list* • *Information that is created whenever you interact with Facebook: such as when you look at another person's profile, send someone a message, search for a friend or a Page, click on an advert or purchase Facebook Credits.*	*er web pages that are connected to Facebook or in collaboration with it.* • *Facebook collects data from our advertising partners, customers and other third parties. Those are data which help Facebook or its partners to better place advertisements.* • *Facebook allows a wide range of advertising network to track your activity on Facebook in order to evaluate placed advertisements. This is why little files, so called "cookies" are stored on your hard disk.*

IQ28. What do you think when all that data about you is collected for advertising purposes? *(relates to RQ 1.3, H 3a)*

PROBING:

Do you perceive this form of advertising as an intrusion into your privacy or as a critical form of surveillance?

What do you think about the fact that FB collects information on other websites for advertising purposes?

IQ29. Is it OK that FB collects these data as long as it is free? *(relates to RQ 1.3, H 3a, RQ 1.4)*

PROBING: Would you pay for FB or other SNS, if they wouldn't use your data for advertising?

IQ30. Assumed that a SNS provider would pay you money or provide you special features on the site, if you would allow using personal data for advertising purpose explicitly, would such a "deal" be interesting for you? Why? *(relates to RQ 1.2, H 2d)*

PROBING IF NOT EXPLICITLY REFUSED: In which case would it be interesting for you?

FB's terms of use (from 25.03.2011, point 10) say "about Advertisements and Other Commercial Content Served or Enhanced by Facebook" that it is FB's "Our goal is to deliver ads that are not only valuable to advertisers, but also valuable to you (...)You understand that we may not always identify paid services and communications as such". The default account settings enable that FB is allowed to use so called "social adverts", which include a personal reference to you or your friends, such as a picture of you and your name. For example a product is displayed together with the statement "NAME likes PRODUCT" and a picture of you is made visible within that advertisement. Social adverts can also be placed on other websites that cooperate with FB.

In the FB's account settings, under the category "Facebook Adverts" it is stated "about Advertisements and Other Commercial Content Served or Enhanced by Facebook" that "Everyone wants to know what their friends like. That's why we pair adverts and friends — an easy way to find products and services you're interested in, based on what your friends share and like." The default account settings enable that FB is allowed to use so called "social adverts", which include a personal reference to you or your friends, such as a picture of you and your name. For example a product is displayed together with the statement "NAME likes PRODUCT" and a picture of you is made visible within that advertisement. Social adverts can also be placed on other websites that cooperate with FB.

IQ31. FB obviously holds the view that users have an interest in such targeted social adverts. What do you think about this? *(relates to RQ 1.3, H 3a)*

PROBING: You can disable social adverts within the account settings. What do you think about this possibility?

In general there are two possible ways to organize users' commitment to the use of their data for advertising purposes. The so called opt-out modus means that you have to disable the usage actively whilst all different opportunities to use your data for advertising are enabled by default. The opt-in modus is the very opposite; here you have to enable first, before data can be used for advertising.

IQ32. What do you think of the so called opt-in modus for the use of your data for advertising purposes? *(relates to RQ 1.3, H 3a, RG 1.2, H 2b)*

PROBING: Should the opt-in modus be introduced mandatory for all SNS provider by law? Why?

During my interviews so far, one interviewee stated that is wrong that the owners of SNS, like Mark Zuckerberg, CEO of FB, gain profits by selling personal data to advertisers, whereas the users have no share in these profits. According to that argument, the interviewee asks why this is not the case revealing personal data on SNS because one normally deserves wages for work.

IQ33. How are you thinking about this line of argumentation? Why? *(relates to RQ 1.2, H 2d, RG 1.3, H 3a)*

IQ34. Do you know or can you imagine alternate forms of funding SNS? What do you think about them? *(relates to RQ 1.3, H 3b)*

PROBING: What do you think about public funding of SNS by taxes or fees, as it is practiced in the context of public broadcasting? What do you think about funding SNS by

donations, as it works for Wikipedia? What do you think about funding SNS by a subscription model, as it works for newspapers and magazines?
At present a few alternate SNS that aren't financed by advertisements exist.
IQ35. Do you know such alternatives? Are you familiar with them? Can you describe them? *(relates to RQ 1.3)*
I want to tell you about two, relatively well-known, alternatives, namely the Diaspora project and kaioo. In the case of Diaspora, it is attempted to avoid that user data are stored centrally; rather it works on behalf of many different private interacting servers. Diaspora is itself a kind Internet within the Internet. In terms of privacy protection, Diaspora promises highest possible control of user data, the opt-in modus is fully realized here. Diaspora will not sell any user data to advertisers; its development was funded by donation as far. The same extends to kaioo. It is a state approved non-profit organization. In the case of kaioo, users can decide themselves about the terms of use and privacy policy on behalf of participating in a Wiki.
IQ36. What do you think about these alternatives as a whole or about single alternate aspects in comparison to FB? *(relates to RQ 1.3)*
IQ37. Would you spend money for such alternate SNS, like Diaspora or kaioo? *(relates to RQ 1.3)*
PROBING: Approximately, how much a year?
IQ38. How do you think such alternate SNS can be financed? *(relates to RQ 1.3, H 3b)*
PROBING: What about public funding? What about the subscription model? What about donations?
DEBRIEFING
We are now at the end of the interview.
IQ39. Are there any open questions which arose during the interview? Would you like to add a point?
Thank you very much for your participation and giving these interesting answers.

Table 2: Final version of the interview guide that was used in the study (changes if necessary due to Facebook's changed terms of use/ privacy policy appear in the left column)

3.3. Data analysis procedures

We applied qualitative content analysis to analyse our transcribed interview data (Kracauer 1952; Ritsert 1972; Mayring 2002; 2004; Schmidt 2004). Qualitative interviews generally allow people to provide information using their own terms, meanings, and understandings. Thereby we focused on analysing the content of the interviews more than observations during the interviews. Systematic qualitative content analysis faced the disadvantage that qualitative research provides less standardization and comparability by providing an intersubjectively understandable coding guide.

3.3.1. Transcription

As we were mainly interested in exploring the interviewee's lines of argumentation, only verbal behaviour was selected to be transcribed; from the same reason we chose to represent the audio material written in standard orthography as deviations of standard orthography do not play a role for identifying lines of argumentation (Kowal and O'Connell 2004, 249-250). Functionally the transcriptions of the audio-taped interviews were done on behalf of the computer program "F4". The first interviews were transcribed completely, then, as the same main questions were asked to each participant, interviewer passages referring to the interview guide were shortened by using catchphrases. Additionally, clearly identified rephrasing within the interviewee's answers were skipped or also marked by catchphrases. Sometimes advices for coding and categorisation were noted within the transcript; however these notes

were clearly distinct from the spoken material in order to prevent counting them as objective measures (Kowal and O'Connell 2004, 251).

3.3.2. Qualitative content analysis

Content analysis is geared towards "to discover new hypotheses, to test a hypothesis in a single case, to distinguish between conceptual terms, to arrive at new theoretical considerations or to revise existing theoretical frameworks" (Schmidt 2004, 257). Our cases were single interviewees, groups of interviewees, lines of arguments, or constellation of lines of argument.

Three ways of analysing content that has been applied in our study can be differentiated. First, we analysed the manifest meaning content of our interviews: Which arguments do interviewees provide us in favour of privacy and against surveillance on SNS, for instance? Second, we analysed the latent meaning contents (Kracauer 1952). In that context we could make a further difference. On the one hand, within a narrow contextual analysis of the latent content, we analysed a certain interview passage by referring to the direct textual environment (that passage in context of the whole interview) or by referring to the other interviewees' textual data. For example, a certain passage about privacy only becomes clear if interviewee's applied arguments against surveillance are considered. On the other hand we really went "beyond the text" (Mayring 2004, 269) by using our theoretical background for data analysis.

Jürgen Ritsert (1972; see also Mayring 2004, 267) suggest how content analysis, which refers "beyond the text", can be applied to critical theory. Referring to contexts beyond the concrete interview data means not only taking the interviewee's social background or the specific interview setting into consideration, but also uncovering aspects of interview data, within which society in its entity appears. This means not interviewees' references to (current) societal events, such as statements about the economic development of society (in the context of digital capitalism, for instance); rather it means identifying societal connotations by the researcher (Ritsert 1972, 41-44). Adorno states in accordance with our methodological starting point: "Society appears as whole behind each concrete social situation" (1972, 145). Additionally, "societal totality does not lead a life of its own over and above that which it unites and of which it, in its turn, is composed. It produces and reproduces itself through its individual moments. (...) This totality can no more be detached from life, from the cooperation and the antagonism of its elements than can an element be understood merely as it functions without insight into the whole which has its source [Wesen] in the motion of the individual himself. System and individual entity are reciprocal and can only be apprehended in their reciprocity" (Adorno 1976c, 109). For our purpose, we wanted to uncover aspects of the political economy of privacy and surveillance within the interview data (figure 1). In this context we were for instance interested in arguments made by users where they adopt interests of commercial SNS and do not show a conscious about being, exploited, other-directed, alienated etc.

Quantifying the encoded answers and arguments given by the interviewees is also part of qualitative content analysis: "Quantifying surveys of material are of particular

value in the preparation of further analysis; they point to possible relationships that can be pursued in a qualitative analysis" (Schmidt 2004, 257). Such quantitative explorations cannot be results per se within a qualitative approach; rather they work as indicators where and how detailed interpretation should be stepping in. Quantitative analysis were accompanied by detailed interpretations of selected out-standing interview passages in order "to discover new hypotheses, to test a hypothesis on a single case, to distinguish between conceptual terms, to arrive at new theoretical considerations or to revise existing theoretical frameworks" (Schmidt 2004, 257).

Coding

Operationalisation in qualitative research, in our case developing a coding guide for content analysis, comes up with the analysis of data, and not before as in quantitative research. It is finished not until analysis is finished. Coding and the development of the coding guide happened in two directions within an iterative process (Mayring 2004, 269; 2000). First direction is "coding up" (J. Fielding 1993, 227). This means developing categories from the transcribed interview data, either as new categories or as a specification of the theoretical assumptions that were implicated in our research questions and hypotheses. Second direction was "coding down" (J. Fielding 1993, 227); here categories were derived from our theoretical framework and our hypotheses. The interchange between these two directions (coding up and coding down) is "continued by contrasting the topics and individual aspects in the interviews with the ideas for categories previously developed" (Schmidt 2004, 255). Thereby it was important to make sure that the development, which will result from that interchange, is made explicit (Ritsert 1972, 87).

To make qualitative coding intersubjectively understandable, we developed a coding guide with a threefold structure. The coding guide contained a list of all issues and (sub-)categories that are consecutively numbered as well as a practical description of each item (see table 3). When it comes to the most concrete categories that contain single arguments or lines of argumentation, the residual category "other" is not displayed here in table 3 in order to save space.

Category number	Category name	Category description
1	ATTITUDES TOWARDS CERTAIN KINDS OF SURVEILLANCE ON SNS	
1.1	Evaluation of the term surveillance	*Interviewees, when they think of surveillance, value the term differently.*
1.1.1	Positive evaluation	*Interviewees think that surveillance is a positive thing as it ensures security, for instance.*
1.1.2	Negative evaluation	*Interviewees think that surveillance is a negative thing as it exercises manipulation and control over people, for instance.*
1.1.3	Ambiguous evaluation	*Interviewees see positive as well as negative aspects of surveillance.*
1.2	Reference to privacy in the discussion of different kinds of surveillance	*Interviewees mention the term privacy in their discussion and valuation of the term surveillance*
1.2.1	Yes	*Interviewees refer to privacy in their discussion and valuation of surveillance*
1.2.2	No	*Interviewees do not refer to privacy in their discussion and valuation of surveillance*
1.3	visible kinds of surveillance/ first association of the term surveillance	*Which kinds of surveillance interviewees think of, when they hear the term surveillance*
1.3.1	State surveillance	*Interviewees name instances of surveillance performed by states, such as secret service or police surveillance, or census measures etc.*
1.3.2	Economic surveillance	*Interviewees name instances of surveillance performed by economic entities, such as corporations or managers.*
1.3.3	Surveillance performed by employers	*Surveillance performed by actual or potential employers*
1.3.4	Surveillance for advertising purposes	*Surveillance performed for advertising purposes, such as targeted advertising*
1.3.5	Individual surveillance	*Interviewees name forms of surveillance performed by individuals, such as criminals, or members of peer groups etc. Examples are also forms of lateral surveillance.*

1.3.6	Surveillance technologies	*Interviewees, when they think of surveillance name certain technological means to surveil, such as video cameras, algorithms etc.*
1.4	Influence of asymmetrical power relations on attitudes towards the term surveillance	*Who is watching and how much power is attributed to a surveiling entity determines interviewees' attitudes towards surveillance.*
1.4.1	Power sensitive surveillance notion	*Interviewees think that power inequality and social hierarchies play a role whether watching is perceived as a problematic form of surveillance. Top-down surveillance is perceived as negative. Whereas bottom-up surveillance and lateral surveillance tends to be seen as positive.*
1.4.2	Power in-sensitive surveillance notion	*Interviewees think that power inequality and social hierarchies does not play a role whether watching is perceived as a problematic form of surveillance. There is no difference in valuation according top-down, bottom-up, and lateral surveillance.*
1.5	Employer surveillance	*Surveillance performed by actual or potential employers*
1.5.1	Awareness of employer surveillance	*Interviewees' awareness, including direct or indirect experiences with surveillance performed by actual or potential employers*
1.5.1.1	Yes	*Interviewees are aware of employer surveillance, have direct or indirect experiences with it and reckon on it when the use SNS.*
1.5.1.2	No	*Interviewees are not aware of employer surveillance, have no direct or indirect experiences with it and do not reckon on it when the use SNS.*
1.5.2	Attitudes towards employer surveillance	*Interviewees attitudes towards employer surveillance*
1.5.2.1	worry	*The degree interviewees are worried about employer surveillance*
1.5.2.1.1	Yes	*Interviewees are worried about employer surveillance (despite they may have used the privacy settings or have limited their data disclosure).*
1.5.2.1.2	no	*Interviewees are not worried about employer surveillance*
1.5.2.1.2.1	Privacy settings/ limited disclosure	*Interviewees argue that they do not worry because they do limited data disclosures and/or use the privacy settings to protect them from employer surveillance.*
1.5.2.2	Agreement/disagreement	*The degree of agreement of employer surveillance*
1.5.2.2.1	Agreement	*Interviewees agree with employer surveillance*
1.5.2.2.1.1	SNS are platforms of self-presentation and self-advertising	*Interviewees argue that surveillance performed by employers is legitimate as users use SNS for purposes of self-presentation and self-advertising also towards actual or potential employers.*
1.5.2.2.1.2	legitimate economic interest of employers	*Interviewees argue that surveillance performed by employers is a legitimate economic interest to evaluate actual or potential employees.*
1.5.2.2.1.3	employer surveillance shows no effect	*Interviewees argue that surveillance performed by employers shows no effect to them. For instance as they are currently students and not looking for a job, they are in a good relationship with the employer, or they point to privacy setting/limited disclosures they have made in order to be protected from employer surveillance*
1.5.2.2.2	disagreement	*Interviewees dislike and do not agree with employer surveillance.*
1.5.2.2.2.1	results in discrimination	*Interviewees argue that surveillance performed by employers results in various forms of discrimination.*
1.5.2.2.2.2	privacy invasion	*Interviewees argue that surveillance performed by employers is a privacy invasion.*
1.5.2.2.3	ambiguous	*Interviewees neither clearly dislike and do not agree nor agree with employer surveillance.*
2	USERS' NOTION OF PRIVACY	
2.1	The value of privacy	*Passages that express interviewees' valuation of the term privacy and give reasons why SNS users value or do not value privacy.*
2.1.1	Non-value	*Passages that express critique of the value of privacy and argue that privacy harms the public interest.*
2.1.2	Values	*Passages that express why interviewees value privacy.*
2.1.2.1	Relief/ withdrawal/ reflection/ silence/ protection	*Interviewees argue that privacy is valued as it ensures silence, regeneration, concentration, protection, time for (self-)reflection and thinking, and relief, for instance from others' evaluation, societal norms, or unwanted negative consequences.*
2.1.2.2	intimacy	*Interviewees argue that privacy is valued as it enables intimacy.*
2.1.2.3	Impression management	*Interviewees argue that privacy is valued as it enables impression management that is consciously decide which aspects of personality are showed to whom.*
2.1.2.4	freedom	*Interviewees argue that privacy is valued as it ensures freedom, such as decisional freedom, or freedom of opinion.*
2.1.2.5	Trust	*Interviewees argue that privacy is valued as it has to do with trust.*
2.1.2.6	respect	*Interviewees argue that privacy is valued as it has to do with respect.*
2.2	Realms or aspects of life that are considered being private or not being private	*Interviewees argue that there are certain realms that are or should be private on the one hand, and that there are certain limits to privacy, on the other hand.*
2.2.1	Private realms	*Realms or aspects of life that are private in the view of interviewees or where they usually find privacy.*
2.2.1.1	Close relationships	*Interviewees argue that close relationships, such as life partner, family, and friends, are private realms.*
2.2.1.2	home	*Interviewees argue that the home and the "own four walls" are private realms.*
2.2.1.3	Financial or business information	*Interviewees argue that financial or business information, such as account information, or information relevant to competition, are private realms.*
2.2.1.4	Ideology and thoughts	*Interviewees argue that the own ideology (religious, political etc.) or more general the own thoughts are private realms.*
2.2.1.5	Body	*Interviewees argue that the own body is a private realm.*
2.2.1.6	nature	*Interviewees argue that the nature is a private realm.*
2.2.2	Scope of privacy	*Passages that express how interviewees think about the scope of privacy.*
2.2.2.1	There are limits to privacy	*Interviewees express that they see limits to privacy.*
2.2.2.2	There are no limits to privacy	*Interviewees say that there are no limits to privacy.*
2.3	Who should define what should be kept private on SNS	*In response to IQ9 interviewee express who should define what should be kept private on SNS.*
2.3.1	individual	*The individual should define what private data are on SNS.*
2.3.1.1	Youth protection	*The individual should define what private data are on SNS, but non-adults are not able to do this and should therefore be protected by society.*
2.3.2	social	*Society or people together should define, for instance by laws, what should be kept private on SNS.*
2.3.3	ambiguous	*Interviewee expresses that both, society/ people together and the individual should define what should be kept private on SNS. Interviewees not only mention youth protection as a case when society should define what privacy is but also mention further instances, such as the protection of non-literate SNS users.*
2.4	Evidence for social or trans-subjective notions of privacy	*Interviewees express in their general reflection about the meaning of privacy aspects of a social or trans-subjective notion of privacy. They express that there are or should be social or trans-subjective instances who define what privacy is. Instances are the cultural determination or privacy or any other passages where interviewees reflect that it is not or not only the single individual that determines privacy.*
3	VISIBILITY OF ADVERTISING ON SNS	*Degree of how visible advertising on SNS appears to the interviewee. This includes the interviewee's awareness of advertising on SNS and her or his knowledge about how it works, the interviewee's awareness of the terms of use and privacy policy within which advertising on SNS is described, and to what extent the interviewee thinks that advertising determines the SNS to any extent.*
3.1	Awareness of the terms of use and privacy policy	*Interviewee's awareness of the SNS's terms of use and privacy policy within which the employment of advertising is described, including the direct or indirect (e.g. via user posts on the SNS or media coverage) witnessing of changes in these documents.*
3.1.1	No awareness	*Interviewee has neither read the documents nor witnessed any changes of them.*
3.1.2	Low awareness	*Interviewee has witnessed changes in the documents but has not read them.*
3.1.3	High awareness	*Interviewee has read the documents at least partly and witnessed changes of them.*
3.2	Degree of knowledge about how advertising	*Degree of knowledge about how advertising works on SNS the interviewee has, including his or her aware-*

	works	*ness that there is advertising on SNS.*
3.2.1	no knowledge	*Interviewee is not aware that there is advertising on SNS at all.*
3.2.2	Low knowledge	*Interviewee is aware that there is advertising on SNS but do not know more about how advertising works or holds wrong assumptions about it.*
3.2.3	Medium knowledge	*Interviewee knows that advertising on SNS is personalised or targeted but do not know more about targeting works or holds wrong assumption about it.*
3.2.4	High knowledge	*Interviewee provides correct descriptions how personalised or targeted advertising works SNS; he or she may hold some additional wrong assumptions about it.*
3.3	Perceived influence of advertising on SNS	*Interviewee's perception if and to what extent advertising influences or determines in any way the appearance or/ and functionalities of SNS, including presence of commercial activities on the SNS (e.g. profiles of brands, other marketing activities).*
3.3.1	Advertising influences SNS to any extent	*Interviewee sees that advertising and advertising related commercial activities influences the appearance and/ or the functionalities of the SNS at least to some extent.*
3.3.2	Advertising does not influence SNS	*Interviewee does not think that advertising and advertising related commercial activities influences the appearance and/ or the functionalities of the SNS.*
4	ATTITUDES TOWARDS ADVERTISING ON SNS	
4.1	Attitudes towards advertising on SNS	*Interviewee's attitude towards advertising on SNS, including their attitudes towards advertising in general.*
4.1.1	Agreement	*Interviewees agree that SNS providers place advertisements on the SNS site.*
4.1.1.1	no negative consequences	*Interviewees argue that advertising and advertisements show no negative consequences for them because they are not forced to notice advertisements, to click on them, and to buy advertised products ultimately. Moreover, they argue that they are not forced to participate in SNS.*
4.1.1.2	positive consequences	*Interviewees argue that advertisements on SNS show positive consequences for them, such as that they provide useful product information and interesting offers, that it is fun watching them, and that advertising makes the usage of SNS free for them.*
4.1.1.3	recognised funding model	*Interviewees argue that advertising is a common and societal recognised funding model and we all are used to have it.*
4.1.2	Disagreement	*Interviewees disagree that SNS providers place advertisements on the SNS site.*
4.1.2.1	negative consequences	*Interviewees argue that advertising on SNS shows negative consequences for them. For instance they argue that it is deflecting, annoying, pressing, manipulating, and creates (unwanted) new needs.*
4.1.2.2	no positive consequences	*Interviewees argue that advertising shows no positive consequences for them and that it is unnecessary and a waste of time.*
4.1.2.3	contradicts SNS' goals	*Interviewees argue that advertising contradicts SNS's inherent and real goal that is about maintaining and establishing social relations.*
4.1.2.4	Discontent about a lack of alternative	*Interviewees argue that there is no alternative to this funding model to choose.*
4.1.3	Ambiguous	*Interviewees take up an ambiguous position towards advertising on SNS; neither agreement nor disagreement can be identified clearly.*
4.2	Use of ad-blocker software	*Interviewees give information that s/he is using ad-blocker computer software that makes certain forms of advertisements invisible.*
4.3	Attitudes towards advertising on SNSs as a privacy invasion or a problematic form of surveillance	*Interviewees' attitudes towards advertising on SNS being or being not a privacy invasion or a problematic form of surveillance.*
4.3.1	Advertising on SNS is a privacy invasion or a problematic form of surveillance	*Interviewees hold that advertising on SNS is privacy invasion or a problematic form of surveillance.*
4.3.1.1	No informed consent	*Interviewees argue that there was no informed consent to advertising. For instance, they argue that that it is not obvious that privacy settings do not apply for advertising, or they terms of use/ privacy policies are unclear.*
4.3.1.2	Disproportion	*Interviewees argue that advertising on SNS is a problematic form of surveillance as it is too excessively and disproportionally performed by the SNS provide. For instance using data collected from other websites is perceived as a privacy invasion.*
4.3.1.3	indirect negative consequences	*Interviewees argue that advertising on SNS shows indirect consequences because the data collected for this purpose can be accessed by third parties, such as state authorities or hackers, later on.*
4.3.1.4	Uncertainty about consequences	*Interviewees argue that they are uncertain about the exact use of their data and this uncertainty is linked to potential consequences for them. In this context they are also afraid that SNS will collect and use ever and ever more data in the future.*
4.3.2	Advertising on SNS is not a privacy invasion or a problematic form of surveillance	*Interviewees deny that advertising on SNS is privacy invasion or a problematic form of surveillance.*
4.3.2.1	informed consent	*Interviewees argue that there was an informed consent by the user to the SNS's terms of use, which also includes the acceptance of targeted advertising.*
4.3.2.2	no negative consequences	*Interviewees argue that advertising on SNS shows no negative consequences for users. For instance, the single user cannot be identified by third parties.*
4.3.3	Ambiguous	*Interviewees take up an ambiguous position towards advertising on SNS as a privacy invasion or a problematic form of surveillance; neither agreement nor disagreement can be identified clearly.*
5	COMMODIFICATION OF PRIVACY	
5.1	Attitudes towards selling personal data in exchange for money or "premium options"	*Interviewees' attitude towards exchanging his or her personal data for money or "premium" options on the SNS*
5.1.1	should not be for sale	*Interviewees state that privacy, personal data should by no means be sold*
5.1.2	can be sold	*Interviewees basically state that privacy, personal data can be sold*
5.1.3	ambiguous	*Interviewees take up a ambiguous position whether personal data should be or should not be sold*
5.2	Attitudes towards compensation payments to the users	*Interviewees' attitude towards the proposal that SNS provider should paythe users for using their personald data in order to gain profit*
5.2.1	Wants compensation	*Interviewees want financial compensation for using his or her personal data.*
5.2.1.1	exploitative ratio between benefits and profits	*Interviewees argue that they see a bad or exploitative ratio between the SNS's profits and their own benefits of using the SNS.*
5.2.2	Does not want compensation	*Interviewees do not want financial compensation for using his or her personal data.*
5.2.2.1	already received compensation	*Interviewees argue that they have already received compensation in the form of the SNS service that provides them with several advantages and benefits.*
5.2.2.2	Legitimate behaviour	*Interviewees argue that the SNS provider behaves completely legitimately. For instance they argue that the SNS's founders had a good idea or good luck, that it is the way things simply are, and that there is no coercion that forces people to be on SNS.*
5.2.2.3	Personal data should not be traded	*Interviewees argue that personal data should not be traded at all and that receiving compensation will not stop this trade; rather any compensation payment is based on such trading.*
5.2.3	ambiguous	*Interviewees take up a ambiguous position whether SNS provider should or should not pay compensation for using personal data in order to gain profit*
5.3	Perception that using the SNS is work	*In context of IQ33 we provided interviewees with an analogy between using SNS and labouring. Interviewees express how they think about this analogy.*
5.3.1	Using the SNS is not working	*Interviewees do not support our provided analogy between using the SNS and labouring.*

5.3.2	Using the SNS is working	*Interviewees support our provided analogy between using the SNS and labouring.*
6	PRIVACY AND USER BENEFITS	
6.1	User benefits	*Interviewees explain why they use SNS and which benefits they gain from that usage.*
6.2	Privacy user-benefits trade-off strategies	*Interviewees compare privacy and surveillance issues and user benefits, which they gain from their usage of SNS.*
6.2.1	benefits of SNS outweigh the surveillance and privacy threats	*Interviewees argue that user benefits outweigh privacy and surveillance concerns.*
6.2.1.1	Privacy settings	*Interviewees argue that they do privacy settings.*
6.2.1.2	Limited disclosure	*Interviewees argue that they limit their data disclosure. This includes that they do constrain their SNS usage.*
6.2.1.3	Subversive usage	*Interviewees argue that they apply subversive strategies, such as making false statements, using pseudonyms or separate email addresses, and propagating critical, "subversive" information about the SNS on the SNS. Subversive information is for instance information about effective privacy protection opportunities, about SNS caused censorship, or about alternative SNS.*
6.2.2	surveillance and privacy threats outweigh the benefits of SNS	*Interviewees argue that privacy and surveillance concerns outweigh user benefits.*
6.2.3	Reflexion on the preconditions of privacy-user benefit trade-offs	*Interviewees reflect about the conditions of their trade-off strategies, such as that the trade-offs are preliminary or that the feel not free in doing the trade-off.*
6.2.3.1	Heteronomy of privacy-user benefit trade-offs	*Interviewees express that they do not feel free in doing trade-offs between user benefits and privacy/ surveillance concerns.*
6.2.3.1.1	no informed consent	*Interviewees argue that they have a lack of knowledge about how their data is processed exactly and that there was no informed consent to the SNS' terms of use and privacy policy.*
6.2.3.1.2	dependency on SNS	*Interviewees argue that it is impossible to waive all the social contacts and relations because it would denote a social exclusion for them.*
6.2.3.1.3	powerlessness	*Interviewees argue that they are powerless because there is only in or out and no real opportunity to make differentiated decision, such as an opt-out opportunity for advertising. The SNS also burdens all the responsibility to protect privacy on the user.*
6.2.3.1.4	Lack of alternatives	*Interviewees argue that there is a lack of alternatives to Facebook's monopoly and they have no freedom to choose between SNS.*
6.2.3.1.5	fatalism	*Interviewees argue fatalistically. For instance, they argue that that nothing is for free in life, that the situation will always be like it currently is, and that they as members of the Internet generation are simply used to give up privacy and to accept surveillance.*
6.2.3.2	Dynamic nature of trade-off	*Interviewees express that their trade-off strategies are preliminary. They argue for instance that their trade-offs will change when their life situation changes, that the positive outcome of the trade-off is quite fragile, and that negative publicity will alter the trade-off.*
7	ATTITUDES TOWARDS PRIVACY PROTECTION ON SNS	
7.1	Attitudes towards privacy protection through the SNS provider	*Interviewees express their attitude towards privacy protection through the SNs provider, including their attitude towards the privacy policies and terms o use.*
7.1.1	Positive	*Interviewees argue that their privacy is well protected by the SNS provider.*
7.1.1.1	no negative experiences	*Interviewees argue that they have made no negative experiences and therefore conclude that the SNS provider protects their privacy well.*
7.1.1.2	SNS provider are controlled	*Interviewees argue that SNS providers are exogenously controlled, for instance changes in the terms of use and privacy policies are adaption to the law or taking place due to public pressure.*
7.1.1.3	privacy needs are taken seriously	*Interviewees argue that SNS providers take their privacy needs seriously because SNS have implemented differentiated privacy setting opportunities, steadily take care of improving the site, voluntarily subject themselves to data protection rules, and try to meet user complaints.*
7.1.2	Negative	*Interviewees argue that their privacy is not well protected by the SNS provider and interviewees mention point of critique.*
7.1.2.1	No privacy in the Internet	*Interviewees argue that privacy cannot be ensured in the Internet in principal; therefore SNS providers' privacy protection must be deficient.*
7.1.2.2	SNS provider are not controlled	*Interviewees argue that the SNS are not controlled either by the participation of users or external institutions.*
7.1.2.3	dishonesty	*Interviewees argue that SNS behave dishonestly and non-truthful, in fact they do not want to protect user's privacy.*
7.1.2.4	In-transparency	*Interviewees argue that the SNS do not make clear what they do with the user data or how users can protect their privacy. The terms of use and privacy policy is not understandable and the SNS do not inform the users about changes of these documents appropriately.*
7.1.2.5	Profit orientation	*Interviewees argue that SNS' profit orientation inhibits effective privacy protection.*
7.1.3	ambiguous	*Interviewees show an ambiguous attitude towards privacy protection through the SNS provider. They argue that the SNS provider protects their privacy but also mention points of critique.*
7.2	Recommendations in respect to the terms of use and privacy policy	*Interviewees mention points/ issues that should be included in SNS's terms of use and privacy policy.*
	informed consent to changes	*Interviewees argue that SNS should ensure that there is a informed consent to changes on the SNS.*
	deleting of data	*Interviewees argue that they wish a deleting of data after a certain period of time or of old data after changes were made.*
	no statistical analysis	*Interviewees argue that the SNS should not do statistical analysis of the users' data*
	No disclosure to third parties	*Interviewees argue that the SNS should not disclose data to third parties, including the selling of personal data.*
	Usage of data only for the genuine SNS	*Interviewees argue that personal data should not appear elsewhere than on the genuine site.*
	ownership of uploaded data	*Interviewees argue that the user should remain perfect ownership of uploaded data*
	clear and concise terms of use and privacy policies	*Interviewees argue that wish clear and concise terms of use and privacy policies.*
	traditional instead of targeted advertisements	*Interviewees argue that the SNS should make use of traditional instead of targeted advertisements.*
	no suggestions of potential friends	*Interviewees argue that the SNS makes no own suggestions of potential friends to users.*
	No face recognition	*Interviewees argue that the SNS should not perform face recognition of its users*
7.3	Introduction of opt-in for targeted advertising	*Interviewees' attitudes towards the introduction of an opt-in opportunity for targeted advertising on SNS. Opt-in means that the usage of data for advertising purposes is automatically disabled and the single user can enable it on request.*
7.3.1	Opt-in opportunity for targeted advertising should be introduced	*Interviewees argue that an opt-in opportunity for targeted advertising should be introduced.*
7.3.1.1	User advantages	*Interviewees do not recognize an explicit conflict of interest between them and the SNS providers at this point. They just stress the advantages or reliefs that users would have if the opt-in mode is realised.*
7.3.1.2	Conflict of interests	*Interviewees see a conflict between their interests and the interests of the SNS provider; they clearly reject the SNS providers' interest.*
7.3.1.3	adoption of SNS provider's interest	*In their argumentation in favour of the introduction of an opt-in opportunity, interviewees (partly) adopt the SNS providers' interests.*
7.3.1.1	Opt-in opportunity for targeted advertising should be mandatory introduced by law	*Interviewees argue that an opt-in opportunity for targeted advertising should be mandatory introduced by law.*
7.3.1.2	Opt-in opportunity for targeted advertising should not be mandatory introduced by law	*Interviewees argue that an opt-in opportunity for targeted advertising should not be mandatory introduced by law.*

7.3.2	Opt-in opportunity for targeted advertising should not be introduced	*Interviewees argue that opt-in for targeted advertising should not be introduced.*
8	ALTERNATIVE SNS	*Our study is also interested in emancipatory alternatives to surveillance, exploitation etc. on SNS. Therefore we asked interviewees about their attitude towards alternative SNS. In our context, the alternative quality of SNS is first of all determined by their funding models.*
8.1	Prior knowledge about alternative SNS	*Interviewee has knowledge about alternative SNS prior to the information input regarding this issue during the interview.*
8.1.1	none	*Interviewee has no knowledge about alternative SNS prior to the information input*
8.1.2	low	*Interviewee has noticed that there are alternative SNS, but has no further knowledge about them prior to the information input*
8.1.3	high	*Interviewee has at least some knowledge about alternative SNS prior to the information input. As alternative SNS are relatively uncommon and rarely used, already some knowledge can be interpreted as "high" knowledge in comparison to the average SNS user*
8.2	Attitudes towards alternative funding models	*Interviewees' attitudes towards the presented alternative funding models.*
8.2.1	Public funding	*Interviewees' attitudes towards public funding, for instances by taxes or fees.*
8.2.1.1	Supportive attitude	*Interviewees support the public funding model for SNS.*
8.2.1.1.1	Public interest	*Interviewees argue that there is a real public interest in financing SNS. For instance, SNS are used by so many and public funding would effectively save costs for society because the costs will be less than the total costs generated by advertising.*
8.2.1.1.2	No exclusion	*Interviewees argue that public funding could help to close digital divides and would avoid exclusion, for instance through social sorting.*
8.2.1.1.3	Mandatory requirements	*Interviewees argue that public funding would enable to make mandatory requirements for SNS, such as better terms of use for instance.*
8.2.1.1.4	Non-commercial quality	*Interviewees being critical about commercial SNS argue that that a public funding model would ensure that SNS become non-commercial.*
8.2.1.2	Challenging attitude	*Interviewees challenge the public funding model for SNS.*
8.2.1.2.1	Unfair costs	*Interviewees argue that public funding of SNS is unfair because not everyone uses SNS but the costs have to be afforded by all.*
8.2.1.2.2	no public interest	*Interviewees argue that there is no public interest in establishing SNS because they exist anyway.*
8.2.1.2.3	State influence	*Interviewees argue that public funding would lead to state influence on SNS*
8.2.1.3	Ambiguous attitude	*Interviewees neither clearly support nor challenge the public funding model for SNS.*
8.2.2	Donation funding	*Interviewees' attitudes towards donation funding.*
8.2.2.1	Supportive attitude	*Interviewees support the donation funding model for SNS.*
8.2.2.1.1	Voluntariness	*Interviewees argue that this funding model is based on voluntariness.*
8.2.2.1.2	Mandatory requirements	*Interviewees argue that donation funding would enable to make mandatory requirements for SNS, such open source code of the software, no advertising etc.*
8.2.2.1.3	Social progressive funding	*Interviewees argue that the donation funding model allows social progression.*
8.2.2.2	Challenging attitude	*Interviewees challenge the donation funding model for SNS.*
8.2.2.2.1	Costs	*Interviewees argue that a free opportunity to communicate would get lost.*
8.2.2.2.2	Not worth/ not important enough	*Interviewees argue that SNS as such are not worth or not important enough to pay or donate for them.*
8.2.2.2.3	In-transparency	*Interviewees argue that donations are an in-transparent funding model and would allow the major donors to influence.*
8.2.2.2.4	Free rider effect	*Interviewees argue that donation funding causes a free rider effect and most of the users will not participate in funding.*
8.2.2.2.5	Destruction of the network	*Interviewees argue that with this funding model the number of users would decrease and destroy the network ultimately.*
8.2.2.3	Ambiguous attitude	*Interviewees neither clearly support nor challenge the donation funding model for SNS.*
8.2.3	Pay per use funding	*Interviewees' attitudes towards a pay per use funding.*
8.2.3.1	Supportive attitude	*Interviewees support the pay per use funding model for SNS.*
8.2.3.1.1	Voluntariness	*Interviewees argue that this funding model is based on voluntariness.*
8.2.3.1.2	Privacy protection	*Interviewees argue that pay per use funding would ensure better data and privacy protection because the personal user data would not be used for advertising.*
8.2.3.1.3	fewer costs for all	*Interviewees argue that pay per use funding would mean fewer costs for all participants.*
8.2.3.1.4	Cost transparency	*Interviewees argue that there are always costs (also with advertising), but payment per use would make them transparent and understandable to the users.*
8.2.3.2	Challenging attitude	*Interviewees challenge the pay per use funding model for SNS.*
8.2.3.2.1	costs	*Interviewees argue that a free opportunity to communicate would get lost.*
8.2.3.2.2	Not worth/ not important enough	*Interviewees argue that SNS as such are not worth or not important enough to pay or donate for them.*
8.2.3.2.3	Free alternatives	*Interviewees argue that there will be always a free SNS.*
8.2.3.2.4	Social exclusion	*Interviewees argue that this funding model would results social exclusions because the SNS would be only accessible for the elite or for the rich.*
8.2.3.2.5	Destruction of the network	*Interviewees argue that with this funding model the number of users would decrease and destroy the network ultimately.*
8.2.3.3	Ambiguous attitude	*Interviewees neither clearly support nor challenge the pay per use funding model for SNS.*
8.3	Attitudes towards existing alternative SNS	*Interviewees' attitudes towards the presented alternative SNS.*
8.3.1	Supportive attitude	*Interviewees support the presented alternative SNS.*
8.3.1.1	"real" network	*Interviewees argue that alternative SNS embody the real network idea, which surrounds social relationships and community building instead of other purposes, in particular gaining profit.*
8.3.1.2	No abuse of personal data/ state surveillance	*Interviewees argue that alternative SNS avoid the abuse of personal data and potential state surveillance.*
8.3.1.3	Non-commercial/non-centralised/ no advertising	*Interviewees argue that alternative SNS are non-commercial, free of advertising and therefore do not need centralised power architecture.*
8.3.1.4	Participation/ self-determination/ self-organisation	*Interviewees argue that these alternatives enable participation, self-organisation, and self-determination (more) effectively.*
8.3.1.5	Pluralism	*Interviewees argue that alternative SNS would establish/ maintain pluralism among SNS providers, which is valued positively per se.*
8.3.1.1	Monetary support	*Interviewees argue whether they would or would not support the alternative SNS also monetarily.*
8.3.1.1.1	yes	*Interviewees would support the presented alternative SNS monetarily.*
8.3.1.1.1.1	≤ 10	*Interviewees would spend less or equal 10 Euro a year for the alternative SNS.*
8.3.1.1.1.2	≤ 50	*Interviewees would spend more than 10 Euro but less or equal 50 Euro a year for the alternative SNS.*
8.3.1.1.1.3	> 50	*Interviewees would spend more than 50 Euro a year for the alternative SNS.*
8.3.1.1.2	no	*Interviewees would not support the presented alternative SNS monetarily.*
8.3.2	Challenging attitude	*Interviewees challenge the presented alternative SNS.*
8.3.3	Ambiguous attitude	*Interviewees neither clearly support nor challenge the presented alternative SNS.*
8.4	Challenges for/ doubts about alternative SNS	*Interviewees mention challenges they see for alternative SNS or doubts about them, such as low user numbers or regarding their sustainability.*
8.4.1	Limited number of user	*Interviewees argue that the number of users will be (remain) limited.*
8.4.2	No sustainable funding	*Interviewees argue that the alternative SNS's funding is sustainable.*
8.4.3	No trust in non-commerciality	*Interviewees argue that they do not trust the non-commercial quality of the alternative SNS. They cannot imagine that nobody will capitalise on the alternatives.*

8.4.4	New power structures	*Interviewees argue that new or different power structures will emerge on the alternatives. For instance, major donors or specialists will influence them.*
8.4.5	Superficial Participation/ self-determination/ self-organisation	*Interviewees argue that that participation, self-organisation, and self-determination will turn out to be only formal or superficial.*
8.4.6	No real decentrality	*Interviewees argue that real decentrality cannot be realised, for instance due to technical limitations.*
8.4.7	Disadvantages of decentrality	*Interviewees argue that a real decentralised architecture may be disadvantageous because it provides less control to avoid problematic or "dangerous" content, insecurity, and irresponsibility.*
8.4.8	No consensus among participants	*Interviewees argue that there will be no consensus about the terms of use among the users.*
9	CHANGES OF ATTITUDES DURING THE INTERVIEW IN RESPONSE TO INFORMATION INPUT	*Our study contains a participatory research aspect which includes that Interviewees are provided with information during the interview. This information input can change their attitudes towards certain issues. A previous coded manifestation may no longer fit; rather another manifestation of the same (sub-)category better fits after the information input.*
9.1	Changes of attitudes towards advertising on SNS	*During the interview the interviewee is provided with information how exactly advertising works on SNS and which data are or can be used to personalise advertising on SNS. This information input made the interviewee changing their attitudes towards advertising on SNS. Manifestations are the same as with category 4.1.*
9.2	Changes of attitudes towards advertising on SNS as a privacy invasion or problematic form of surveillance	*During the interview the interviewee is provided with information how advertising exactly works on SNS and which data are or can be used to personalise advertising on SNS. This information input made the interviewee changing their attitudes towards advertising as a privacy invasion or problematic form of surveillance. Manifestations are the same as with category 4.3.*
9.3	Changes of attitudes towards monetary support of (alternative) SNS	*During the interview the interviewee is provided with information about alternative SNSs by using the examples Diaspora and kaioo. This information input made the interviewee changing their attitudes towards monetary support of SNS. Manifestations are the same as with category 8.3.1.1.*

Table 3: Coding guide

In order to develop our coding guide we applied concrete analysing steps that borrow loosely from the approach of "thematic coding" (Kuckarrtz 2010, 84-92; Schmidt 2004). The following step by step procedure was assisted by the computer program "maxqda" (Kuckartz 2010):

Material-oriented formation of analytical categories included an intensive rereading of the transcripts including information that has been noted on the protocol sheets on a case-by-case basis. Theoretical prior knowledge, research questions, and hypotheses guided this reading in order to identify single related topics and individual aspects of these topics that occur in every single transcript. We also noted aspects of topics that do not fit to our conceptual framework immediately. For instance, from our theoretical background (research questions and hypothesis), we were interested in several topics, such as "certain kinds of surveillance", "visibility", "targeted advertising", "alternative funding models", "notion of privacy", "privacy user-benefits trade-offs" etc. Several categories according our topics were already predetermined by our theoretical background. For instance in the context of "certain kinds of surveillance" and the more concrete forms of "targeted advertising" and "surveillance performed by employers" the categories "agreement" and "disagreement" resulted from our research questions. Due to our structured approach no new topics emerged due to the interviews but new aspects did. For instance, interviewees reflected about the conditions within which they do trade-offs between privacy needs and benefits that they gain when they use the SNS. We created therefore a new category "Reflexion on the preconditions of privacy-user benefit trade-offs". Another example in this context was the topic "users' notion of privacy". We had in mind the hypothesis that an understanding of privacy that is based on the control theory is influential among SNS users. The interviews revealed that our operationalisation of this hypothesis (the particular questions that we have included in the interview guide) was not complex enough. This insight resulted in a new discussion about dominant privacy theories.

For category development we contrasted the occurred topics with the ideas for categories developed before and assemble the categories into a guide for coding. At this level the coding guide consisted of issues, categories, and subcategories plus their

descriptions, but has had not yet reached the desired level of concretization. For instance, the category "attitudes towards targeted advertising on SNS" and their subcategories sub-categories "agreement", "disagreement", and "ambiguous" were developed but no categories for the applied lines of argumentation to (dis-)agree existed so far.

First coding of the material according the developed guide: Here the categories "that were established from the material are now applied to the material" (Schmidt 2004, 256). Consequently in this process a loss of information has had to be accepted. The descriptions of categories were proofed in the light of the coded interview passages and it was decided if the analytical category was adequate. We hypothesized that a typical attitude expressed by SNS users is that they are unconcerned about the use of their data for economic ends because this form of surveillance is mainly invisible and does not show direct visible effects. The experiences during the interview process helped us to clarify our implicit assumption about the variable "visibility" and "knowledge" that is supposed to influence peoples' attitudes towards surveillance. Visibility included, in its weakest form, awareness of surveillance; it then included also knowledge of surveillance that can be seen as a stronger form of visibility than awareness; finally it included the visibility of personal consequences that surveillance actually or potentially shows. Whereas visibility could be easily depicted in the coding guide (see categories about awareness of the terms of use and privacy policies, and prior knowledge about how advertising works on SNS), it appears that the question after visible effects or consequences was part of interviewee's lines of argumentation whether they agree or disagree with targeted advertising. At the end of this step, we received an improved coding guide and interview passages attributed to categories and subcategories.

Now we viewed all passages from different interviews according one category or subcategory. We applied fundamental interpretative techniques to this categorical overview. These techniques consisted of paraphrasing, abstraction (finding more abstract categories for instances with the same meaning), reducing passages with the same meaning, and grouping similar passages together and give these groups names that include all instances (Mayring 2010, 70). The process resulted in further (sub-)categories with the desired level of concretization for each existing category/subcategory including their descriptions. At this level we introduced the residual category "other" for passages that we could not attribute to a category. However, while "coding up" we ensured that the residual category was as seldom as possible used for coding. For instance the category "agreement" in the context of "attitudes towards targeted advertising on SNS" received the following manifestations: "no negative consequences", "positive consequences", and "recognised funding model". These manifestations together included all arguments that were employed by our interviewees in this context.

We applied the final coding guide, which was at that time concrete enough, again to the interview material. Thereby we made use of two different forms of coding techniques: First, we were interested in attributing interviewee distinctively to certain

(sub-)category. For instance, we wanted to know if an interviewee either agrees, or disagrees, or shows and ambiguous attitude towards targeted advertising on SNS. In this case just one manifestation was coded for each. Second, we were also interested in exploring influential lines of arguments appearing across the whole sample. For instance, interviewees employed more than one argument in order to express their agreement with targeted advertising. We did not code the most dominant argument but more than one manifestation of the category "agreement with targeted advertising on SNS" was coded.

Analysing steps employed after coding

After the coding process we proceeded with the analysis of the interview material and applied the following steps:

- Quantifying surveys of the material were conducted, that means that the frequency of categories within the material was counted. This gave us an overview which attributions, attitudes, and lines of argumentation were dominant or marginal in our sample. Quantifying surveys were done according categories or per interviewee. For instance one result was that "intimacy" was the most frequently mentioned value of privacy across our sample and 14 out of 30 interviewees held the attitude that targeted advertising is a privacy invasion. A further instance was that all of our interviewees showed supportive attitudes towards introduced alternative SNS and that only one out of 30 interviewees did not want the introduction of an opt-in opportunity for advertising on SNS.
- Attitudes and single lines of arguments were first described and then interpreted on behalf of critical theory concepts, such as exploitation and alienation. For instance, users discontent about the use of their data for advertising purposes through the SNS provider as well as their insistence of compensation payments were interpreted as a marker of exploitation on SNS.
- We could not include all categories in a detailed analysis that goes beyond description and interpretation of description; hence case variables were developed out of several core categories in addition to the variables developed out of the socio-demographic questionnaire. Core categories are categories which we wanted to especially focus on; they were selected according our research interest and they were categories have been distinctively attributed to each interviewee. For instance, the category "attitude towards advertising on SNS" was selected as case variables. Either the value "agreement" or "disagreement" or "ambiguous" were attributed to each interviewee. Attributing case variables to interviewees served as preparation for further quantifying analysis.
- Relations between case variables were explored on behalf of cross tabulation. For instance, we proofed if those interviewees who thought that targeted advertising on SNS is a privacy invasion at the same time supported alternative SNS. The aim here was to explore inductively which combinations between variables arise (not at all, frequently, or rarely) across the sample, but also to test which assumed combinations were found or not found. For instance it was notable that those who do not want compensation in return for the usage of their data through SNS provider also thought that privacy should not be for sale to large

extends. This relation in mind we went back to the interview material and propose a potential explanation for the relation: In both cases privacy must be alienated and alienation is principally not welcomed by this interviewee group.

- One of the aims of qualitative data analysis was to identify types. In our study we differentiate between constructed types and real types. With the first, we use manifestations of categories and assemble types that fit ideal-typically to our theoretical assumption. For instance, we thought about which attitudes must be valid in order to speak about a critical type in the context of economic surveillance on SNS. On the contrary, we thought about the critical type's natural opponent, the uncritical. This way of constructing types is opposed to finding real types in our sample.

4. Results

In the following sections we present results from our study according several topics. First, interviewees' thinking of different kinds of surveillance is dealt with. Second, interviewees' notions of privacy are explored. We ask third for interviewees' attitudes towards advertising on SNS. Fourth, we explore the issues of privacy as commodity and exploitation. Fifth, we deal with interviewees' trade-off strategies between privacy and user benefits, as well as potential alienation they face when they are using SNS. Sixth, we are interested what interviewees think about alternative SNS. Seventh, we report some consequences of the interviews for our interviewees. Eight, we present some user types based on the interview material.

4.1. Different kinds of surveillance

To explore interviewees' notion of surveillance, they were asked to tell us what comes into their mind when they hear the term surveillance (IQ3 and 4). Interviewees' answers allows us to draw conclusions not only about their notion of surveillance (e.g. if it is a more positive or negative phenomena for them), but also which forms of surveillance are particularly visible to our interviewees. Likewise in academic literature, different valuations of the term surveillance also appeared in our interviews. Whereas only 2 interviewees see positive connotations of it, the majority thinks that surveillance is either negative (10 interviewees) or ambiguous (has positive and negative aspects; 9 interviewees hold this opinion). Those who think of surveillance in a positive manner, stress that it enables security and protection from crimes. Interviewee 5 is an example in that context, s/he says:

"Currently, evermore cameras are installed in general, for instance in the innercities and evermore public places are surveiled due to the general security. […]/ Interviewer: If you think about SNS, who can watch you there and to what purpose?/ Well, the provider of the SNS could do that. [In order to] generally check what happens on the platform and perhaps also to report negative things, like any pictures or if anybody is going to meet because they want to bandy."

Those who stress the negative character of surveillance, argue that it is a privacy invasion, secures existing power inequalities through control, exploitation, and manipulation. For instance, interviewee 17 argues in regard to state surveillance:

> *"Theoretically, if the state would represent the common good then surveillance would only be the defence of events that harm the common good. Terrorist attacks, which really are terrorist attacks and affect the lives and health of the citizens in a reasonless way. However, because the state, in fact, has many other interests too, things to protect power relations belong to them. For instance, in the USA the civil rights movement or the women movement was fought against by the FBI and the CIA." Interviewee 16 argues in regard to economic surveillance: "Let's take loyalty cards, for instance. People disclose information voluntarily […], they assume taking advantage from it, getting any special offers or so. […] I assume that many people do not know that corporations have a profit interest to collect these data in order to create targeted advertising from it, for instance. […] Surveillance is based on disclosing data, no matter if knowingly or unknowingly, and then things are made on behalf this data, that one does not want or one is not aware of."*

In our interviews the term surveillance is often seen as neither positive nor negative distinctively; rather ambiguous (with 9 interviewees), which reflects the non-agreement of the various surveillance theories. In this context, interviewee 18 is an example. S/he argues regarding state surveillance and answers the question why state authorities do surveillance:

> *"Surely the first argument from their side is protection or security. This is surely correct to a certain extend. […]. It is protection, but also protection for the state apparatus and not necessarily protection of the rest of mankind."*

What applies to the assessment of surveillance on a general level does not automatically apply to certain kinds of surveillance too. Therefore we explicitly explore some forms of surveillance in our study (see 4.3 and later in this section). However on this general level we are able to propose that pure positive notions of surveillance are empirically little anchored.

Most often interviewees link surveillance to corporations (22 out of 30 interviewee), the state (20 out of 30 interviewees), and in general various technologies that allow certain entities to surveil, such as the Internet or surveillance cameras (14 interviewees). Fuchs (2011b, 142) reminds us that the societal distribution of technological means of surveillance is in favour of the state and (large) companies. In total, 22 interviewees associate economic aspects with surveillance. In their view this includes, workplace surveillance, targeted advertising, loyalty cards, market research, data trading, and surveillance performed by employers. Regarding state surveillance, interviewees mentioned instances, such as surveillance by the police and secret services, surveillance in the health care system, census records, surveillance by the treasury, authoritarian state governments, and counterterrorism laws. State surveillance is obviously visible to our interviewees. More seldom and therefore less visible

to our interviewees, other types of surveillance, such as surveillance in families, surveillance performed by (criminal) individuals (e.g. hackers), and lateral surveillance are mentioned. We can conclude that lateral surveillance is not perceived as a typical form of surveillance.

In order to explore our hypothesis that power inequality and social hierarchies play a role whether watching is perceived as a problematic form of surveillance, we asked interviewees several questions regarding a constructed setting within a lecture at university (IQ13, 14, and 15). Bottom-up surveillance of students can best be exemplified by the academic hierarchy between professors and students. Professors hold the power to grade students, to assign them recognition, and to decide about their future career opportunities. We hypothesize that students welcome to watch their professors on SNS, and so to challenge universities' power hierarchy. Consequently, we hypothesize that when it comes to top-down surveillance, which means that professors watch their students' profiles and activities for instance, students argue for protecting privacy and against surveillance on SNS. In support of our hypothesis, nearly two third (19 interviewees), would only label top-down watching as problematic form of surveillance or privacy invasion, that is when professors watch their students on SNS. Lateral (students watch students) and bottom-up watching (students watch their professors) is not perceived as problematic form of surveillance or privacy invasion by them. Interviewee 12 expresses this when s/he was asked how s/he thinks about a situation within which professors watch their students on SNS:

> *"I would find it weird. I would not feel comfortable if that would be the case. This is because I like to separate University, job, and the private. It would be the same situation as if my boos would surveil me […]./ Interviewer: What would be the difference here in comparison to the other two example situations [students watch each other, students watch their professors]?/ Students are on the same level, but the professor is on a higher level. In the latter case it is not OK, in the former it would be OK; one hast o differentiate according if they are on the same level or if they are able to 'harm' me". Interviewee 13 assists: "It is more like surveillance if your professors are spying you out. It is always so if somebody stands higher in any hierarchy. One feels monitored more likely by a higher authority than by a 'little' student."*

On the contrary, interviewee 10, who apparently has a power relation in-sensitive surveillance notion, answers the question whether the situation when professors are watching their students is a problematic surveillance or a privacy invasion:

> *"I feel it is not surveillance […] I think that professors are just as curious as students. No, [it is not surveillance] as it is again self-chosen." In this case the circumstance that information disclosure is self-chosen renders the situation as a non-surveillance situation. Interviewee 5 argues that there is no difference between the three situational settings, for him/her "surveillance is characterised by a long period of time. Only if somebody is watching a site year-long, then it would be surveillance."*

Our results so far – surveillance is primarily not perceived as a positive thing, lateral watching tend to be not deemed surveillance, surveillance, in the view of users, includes power asymmetries - support Fuchs' line of argumentation (2011b). He argues that the term surveillance should be used as a critical term pointing to societal power inequalities.

case	visible kinds of surveillance/ first association	evaluation of the term surveillance	Influence of asymmetrical power relations on the attitude towards surveillance
1	State surveillance; economic surveillance; surveillance technologies	-	yes
2	State surveillance; surveillance technologies; economic surveillance	-	no
3	-	-	-
4	state surveillance; surveillance technologies; economic surveillance: advertising	negative	yes
5	State surveillance; surveillance technologies; economic surveillance	Positive	no
6	surveillance technologies	-	no
7	State surveillance; surveillance technologies; economic surveillance: advertising	-	yes
8	economic surveillance: advertising	negative	-
9	economic surveillance: advertising, employers	negative	-
10	Surveillance technologies; economic surveillance: advertising	ambiguous	no
11	Surveillance technologies; economic surveillance: advertising; state surveillance; lateral surveillance	negative	-
12	Surveillance in families; state surveillance; individual surveillance	negative	yes
13	State surveillance; lateral surveillance	ambiguous	yes
14	State surveillance; individual surveillance	-	yes
15	Surveillance technologies; economic surveillance: employers	ambiguous	no
16	State surveillance; surveillance technologies; economic surveillance: advertising	negative	yes
17	State surveillance	Negative	yes
18	Surveillance technologies; state surveillance	ambiguous	yes
19	State surveillance; economic surveillance: advertising	ambiguous	yes
20	State surveillance; individual surveillance	ambiguous	yes
21	Economic surveillance: advertising	ambiguous	yes
22	State surveillance; economic surveillance: advertising	positive	yes
23	state surveillance; economic surveillance	-	yes
24	Surveillance technologies; state surveillance; economic surveillance: advertising	negative	yes
25	State surveillance; economic surveillance: employers	-	yes
26	State surveillance	ambiguous	yes
27	State surveillance; surveillance technologies; economic surveillance: employers	-	yes
28	Surveillance technologies; economic surveillance: employers	negative	no
29	Economic surveillance: employers	ambiguous	-
30	State surveillance; surveillance in families; economic surveillance: employers	negative	yes

Table 4: The term of surveillance: visible kinds of surveillance, interviewees' evaluation of the term, and the aspect of power inequalities.

Generally, economic surveillance is an issue that lacks theoretical and empirical research attention (Sevignani, Kreilinger, Allmer, and Fuchs 2011). This situation stands in stark contrast to our interviews that have shown that economic aspects are most frequently linked to the term surveillance. This was the case before we point to this topic in our interviews. These results further back us in focusing our research on economic aspects.

We, then, particularly asked about surveillance performed by employers (IQ4 and 5), may it be within the job applicants screening process or the surveillance at the workplace, when somebody is already employed. This allows us comparing this estimated more concrete form of economic surveillance to the estimated more invisible form of surveillance for advertising purposes.

8 out of 30 interviewees mentioned surveillance by employers, when they were asked what they first link to the term of surveillance. Interviewees associate employer surveillance just as often as they associate advertising with the term surveillance. In a probing question that deals concretely with employer surveillance, nearly all interviewees stated that they are aware of this issue or that they even have direct or indirect experiences with this kind of economic surveillance. We are able to distinct between two dimensions in interviewees' attitudes towards employer surveillance: Cases who are worrying about employer surveillance and those who do not, on the one hand, and between those who dislike employer surveillance and those who find it OK, on the other hand. Along these dimensions, we found three attitudes: Those who find it OK and do not worry; those who dislike it but do not worry; and those who dislike it and worry about it.

Interviewees who find employer surveillance OK and therefore do not worry about it make use of different arguments: They either think that SNS are platforms of self-presentation and self-advertising also in regard to potential or actual employer, or they think that it is the legitimate economic interest to get acquainted with actual or potential employees in order to better evaluate their working efficiency. Interviewee 12 is aware of counter arguments but finally waive them:

> *"Yes, like I said before, if I emphasize the situation, then I think it is more important that employees are watched than to respect their privacy. It is not easy, but like I said, everyone has a right to privacy, but in a way I would say that one also must have control over the own employees."*

A third line of argumentation why users accept this type of surveillance is that they simply state that employer surveillance does not affect them because they are non-working students and not looking for a job, or that they are in a good relationship with the employer. Another argument made here is that SNS's privacy settings or their own information disclosure behaviour protects them effectively from employer surveillance. This argument (which we will explore in more detail below), is the most influential to express that one does agree and is not worried about employer surveillance. It is also applied among those who dislike this form of surveillance, but do not worry. Interviewee 6 argues in that context:

> *"Well, I hide my profile as much as it is possible […] Of course, if somebody could see all that what I usually post, then that would not so good. […]. As I said, the political attitude is easy to identify on it. Perhaps the employer would not be so confident in my case. However, I also think that one worries too much because everyone posts so much on Facebook and the employer may finally find no employees who have a serious profile".*

Those users who dislike employer surveillance apply two lines of argumentation: First, they argue that employer surveillance will result in discrimination (that one does not get a job, or one has disadvantages in the job); second they argue that employer surveillance is not OK as it is a privacy invasion. Those who dislike employer surveillance and are worried about it also apply privacy settings and limited disclosure strategies, but may not fully trust them so that worries remain relevant. We have also found two cases with ambiguous attitude towards employer surveillance. They balance on the one hand the privacy argument, and on the other hand, the argument that employer have a legitimate interest in surveillance. However, otherwise than interviewee 11 above, they finally do not hold the opinion that the economic interest outweighs the privacy issue.

4.2. Notions of privacy on SNS

Before we asked privacy related questions, 20 out of 30 interviewees used the privacy term in their discussions of surveillance in general and of employer surveillance (in response to IQ2-5). After we picked up the privacy issue in the interviews, 16 interviewees argued that surveillance for targeted advertising affects users' privacy (the see that either clearly or were ambiguous). After the information input how advertising works on SNS, the number of those interviewees increased to 25 (see 4.3). These results support the hypothesis that a reference to privacy is relevant in order to argue against surveillance on SNS. We can conclude that users reframe structural issues, such as surveillance, in individual terms, such as privacy (Nock 1993, 1; Lyon 2005, 27; Stalder 2002). On the one hand, we think, the concept of privacy helps users to articulate direct individual consequences of surveillance; on the other hand, consequences of surveillance that are relevant on the macro level of society, such as social sorting, exploitation, lack of democracy, cannot be adequately articulated on behalf of the privacy concept. In the latter case the reference to privacy may block users' understanding of more societal issues in the context of surveillance. Some scholars (see Stalder 2002) argue that referring to privacy cannot be the appropriate way to challenge surveillance effectively. In our study we did not explore the differences between both concepts empirically (see limitations of our study). We presume the equation of privacy invasion/threat and problematic form of surveillance in our instrument. This means that problematic surveillance denotes a privacy invasion.

As there is a theoretical dispute how to define privacy within the literature (Tavani 2008; Schoeman 1984), it is interesting to explore how exactly the reference to privacy is meant and used by SNS users (IQ 6-11). In our study we received answers to the following questions:

- Why do SNS users value or do not value?
- What aspects of life, do they think are private, which limits to privacy do they see?
- Who defines what privacy is? Is it up to the individual or is privacy intersubjectively defined by society?

case	Value or non-value of privacy	Private realms	Privacy limits
1	intimacy, freedom	Nature, home	yes
2	Relief/withdrawal/reflection/silence	Close relationships	yes
3	Protection	home	-
4	Impression management	Home, financial and business information	yes
5	Intimacy, trust,	Close relationships, emotions	yes
6	Freedom	Thoughts and ideology	yes
7	Protection	Thoughts and ideology, close relationships, financial and business information	yes
8	Impression management, intimacy, respect	close relationships	No
9	Relief/silence/reproduction	-	No
10	Impression management, protection	Financial and business information	yes
11	Freedom, Silence/concentration, intimacy	-	yes
12	Trust, intimacy, protection	Close relationships, emotions, leisure time	yes
13	Relief/silence/concentration/time for thinking	Close relationships	No
14	freedom, trust, protection	Close relationships	No
15	Protection, freedom	-	yes
16	Non-value, protection, intimacy	emotions	yes
17	Impression management	Close relationships, emotions	yes
18	Relief/silence/protection	Close relationships	yes
19	Non-value, protection, respect	Body	yes
20	Protection	Home	No
21	freedom, intimacy, protection	-	yes
22	Protection	-	No
23	Respect, protection/concentration	Leisure time	No
24	freedom, trust, silence/protection, impression management	Close relationships	yes
25	Freedom, protection	Home, body	No
26	-	Close relationships	no
27	Intimacy, trust, protection	Close relationships, leisure time	no
28	Intimacy	-	yes
29	Silence/protection, freedom	Home, close relationships, thoughts and ideology	no
30	Non-value, withdrawal/relief/regeneration, intimacy	Home, close relationships	yes

Table 5: Notions of privacy: privacy values, privacy realms, and limits to privacy

Daniel Solove (2009) summarises values commonly associated with privacy and speaks about the following: "intimacy, friendship, dignity, individuality, human relationships, autonomy, freedom, self-development, creativity, independence, imagination, counterculture, eccentricity, freedom of thoughts, democracy, reputation, and psychological well-being" (98). We found empirical evidence for a similar but narrower range of privacy values among our interviewees. Frequently our interviewees named the privacy values freedom (9 times), including decisional freedom and freedom of opinion, and intimacy (10 times), including partnership, family and friendship. Privacy is most frequently valued as it ensures a realm where people can withdrawal to and find silence, regeneration, concentration, protection, time for (self-)reflection and thinking, and relief, for instance from others' evaluation, societal norms, or unwanted negative consequences (20 times). Less frequently, our interviewees argue that privacy enables impression management, that is the value to display different groups of people different aspects of the own identity (5 times), and has to do with trust (4 times) and respect (2 times).

There is also substantial critique of the value of privacy. For instance, Solove (2009, 80-83) names that privacy is threat to community, solidarity, trust, transparency, and security, and that it shields the oppression of women. Three of our interviewees

named that privacy is also a non-value; they argue that privacy shields realms, such as the family, or processes, such as the oppression of women, violence, or other crimes, from political access and generally harms the public interest. Interviewee 19 argues in that context but also connects privacy to the value of freedom:

> *"Basically, it cannot be private when a man hits his wife; he cannot appeal that this happens in a private space. This is due another person is affected. [...] When the line is crossed and not only the own freedom is affected, then consequently privacy has to come to an end." Interviewee 30 assists: "There is this old slogan that the private is political; and it is correct. The private is not completely uncoupled from the general society. Hence a lot of things that happens in a private space are not OK from a societal or human perspective. Frequently this is whitewashed when it is said that my privacy is of no one's business. An instance is violence in the family, against the children or the partner. This has nothing to do with privacy."*

In our study to further explore the meaning of privacy, we found answers to the question not only why interviewees value privacy but also what aspects of life are private for them. Most frequently our interviewees argue that close relationships, such as the partner, family, or friends. One interviewee named face to face communication as private in character, which can be added here (14 times). The home is an important private realm, interviewees speak in this context about the own four walls, and doors to close for instance (7 times). Sometimes interviewees mention financial and business information, such as the income, account balances, purchase information, client relations etc as private information (3 times). Ideology and the own thoughts, such as the political or religious perspective, as well as feelings or emotional problems, are also deemed to be private (each 3 times). More seldom in our sample people point to the body (2 times) and the nature (1 time) as private realms.

Interviewees also provide us with arguments about if and where they see limits to privacy (IQ8). A substantial number of eleven interviewees argue that there should not be any limits to privacy as they think that it is up to the single individual to decide what he or she want to deem private. On the contrary those who mentioned limits to privacy (18 interviewees) basically argued that the public interest can outweigh a right to privacy or that privacy would harm society in some cases. Amitai Etzioni, author of the book "The limits to privacy" (1999), argues that "privacy is a good, but hardly the only one; and privacy must be and is regularly weighed against many other goods" (Etzioni 2005, 253). Therefore privacy "cannot be extended to the point that it undermines the common good; conversely, duties set to maintain social order cannot be expanded to the point that they destroy privacy" (Etzioni 1999, 198-199). Our interviewees mentioned certain instances of the public interest that should set limits to privacy, such as ideas, knowledge, the educational sector, politics in general and politicians in particular, or, frequently mentioned, crimes. Etzioni (2005, 258-259) is also aware that privacy in the economic sphere frequently causes problems for the common good. In this context, interviewee 5 argues that:

"for a person there should be no limits. If somebody wants to disclose really nothing then s/he can do this. This is different with companies. In this case there should be a certain transparency according monetary things but also according appointments." Interviewee 16 extends and radicalises this argument: "I hold the opinion that privacy should not exists for the state, companies, or organisation in the public sphere. This also applies if it has negative consequences for groups, public authorities, organisations, and corporations. With a private person things are more difficult. But if they are linked to any organisations or corporations I would stick with my previous argument. It should be clear that a certain transparency is necessary."

Interestingly, interviewee 5 not only does see limits to privacy for corporations, s/he also point to a more subtle variation of privacy limits. S/he argues:

"I think it should be left everybody free to decide what s/he discloses and what s/he does not disclose. If somebody does not want to disclose his or her age principally or changes his or her name when s/he goes out, then s/he is free to do so. However if this person carries too far then I don't want to deal with this person because it is strange if somebody discloses nothing".

Etzioni (1999) also pleads for communal scrutiny in regard to which extends privacy should be realised in accordance with the common good. We can interpret the quote above, where Interviewee 5 points to social norms, such as role expectations or decency, as an instance for communal scrutiny that regulates and respectively limits privacy.

Interviewee 6 offers another approach to limit privacy by at the same time supporting it. Here, not the common good is acclaimed to limit privacy but the individual privacy interest itself is. S/he argues:

"Normatively, the idea of political liberalism is crucial for me. Hence the idea that all is private as long it does not harm somebody else. This is in analogy to the postulate of freedom that one is as long free until one constrains some other's freedom".

Furthermore, we recognised in our study that some users hold more societal or inter-subjective and some users hold more individual privacy notions. Applied to SNS we asked our interviewees (IQ9):

I am giving you now two statements; can you tell me which one is more appealing to you? Statement 1: Everyone should decide oneself upon which information should be private and which information he/she wants to publish on SNS. Statement 2: There is information that should be always and mandatory for all private and never be public.

Consequently agreement to the first statement expresses an individual notion of privacy; agreement to the second statement expresses a privacy notion that goes beyond individual definitions and is inter-subjective or societal in character. We found

clear individual notions of privacy among 13 interviewees. For instance, interviewee 2 argues this way and reflectively rejects inter-subjective privacy definitions:

> *"I would prefer the first statement due to individual decision-making plays a crucial role in it. There is nothing forced upon one. [...] OK. In the case of nude pictures, for instance... everybody is able to decide how far he or she is willing to make such things public or to keep them private. Or should nude pictures generally remain private and not be published on SNS. [...] That is a difficult thing ... it would make sense to introduce a taboo for pictures, but how far can we go? Nude pictures are only an instance of pictures that should be not allowed. Where to draw the line is unclear. Therefore I would rather say that it should be allowed. Otherwise one have to forbid things that are equally bad for me or others. It must be allowed; there is no clear line. Everybody finds different things offensive."*

Interestingly, 11 interviewees also agree with the first statement but additionally are concerned with youth protection. Interviewee 8 expresses this:

> *"I find it hard to decide as I principally think that everybody must be able to decide on one's own behalf. It should be up to every individual. [...] But if children in the age of 14 make all their private data public on Facebook and they just don't know what they do, then it would be make sense to determine that certain things must be kept secret and are not allowed to disclosed./ Interviewer: You have talked about child and youth protection. Are there any other instances to intervene in individual decisions?/ No, it is mainly about youth protection. I think, as an adult, one should be able to decide."*

We thought about the question whether the recognition of youth protection is really a marker of trans-subjective privacy notions. On the one hand, to expect user data produced by non-adults from the usage for targeted advertising purposes, can be seen as an objective regulation made by society that overrides the individual control of non-adults over their personal data. On the other hand, non-adults appear in this view as individuals who regularly have not yet reached full decision making ability and therefore are generally not fully responsible for their behaviour. They are worth to protect exactly because they are so to say recognised imperfect individuals from this perspective. One can argue that the users' application of inter-subjective privacy definitions in this case presupposes a regular situation where the individual privacy notion would be valid. Interviewees do not reflect on potential constraints that are facing all individuals (including adults) in our society. Therefore we interpret interviewees' exception from the individual privacy definition for non-adults users not as a typical inter-subjective privacy notion and tend to group the respective interviewees together with those who have individual privacy notions. In total 24 interviewees have then individualistic notions of privacy.

We found no clear social definitions of privacy. If interviewees agree with the first statement, but see other or additional reasons to intervene in individual decisions about what should be kept private than youth protection, we interpret this responses

as ambiguous. Examples in this context are that individual privacy decisions should be constraint as there are non-literate SNS users, poorly informed SNS users. Those interviewees do not point to natural reasons (age) but more socially shaped reasons to intervene in individuals' privacy decisions. We found ambiguous, not clearly individual or inter-subjective/societal privacy notions among 6 interviewees. For instance, interviewee 5 supports the first statement but also responses to the question whether there should be laws about which information has to be kept private:

"Yes, I definitely think that pornographic stuff or any videos about brawls, other crimes, and delinquent things should not be allowed to make public on SNS"

Interviewee 29 also agrees with the first statement but, for him/her "the mandatory presetting should be that all is private and later on one can consciously disclose information. [...] Only if things are this way, then everybody should be allowed to decide self-determined."

Interviewee 19 argues also ambiguously: "I see problems with both statements. The truth is in the middle. [...] Mandatory obligations do make sense as I see privacy as a good that not only should exist as a right but also as a real opportunity. On the other hand, when it comes to privacy, one cannot get rid of an individualistic perspective, that means the first statement is also valid. Just as little I welcome a coercive surveillance state, as I welcome a state that forbids citizens to make whatever kind of information public. I do not agree that the state forbids nudism. If people want that, then they should be able. I can introduce certain protections if this is perceived by some as offensive; but it cannot be 100%. If they associate in a network and want to disclose all there, then they should be allowed to do this."

case	Definition of privacy in the context of SNS	Inter-subjective/societal aspects of privacy
1	individual	Culture determines
2	individual	no
3	individual (youth protection)	-
4	individual (youth protection)	equality
5	ambiguous	Social norms and expectations
6	individual (youth protection)	Culture determines, average of individual privacy needs
7	individual	no
8	individual (youth protection)	Privacy relies on the acceptance of others
9	individual	no
10	individual	no
11	individual (youth protection)	no
12	individual	no
13	individual	no
14	ambiguous	Public interest: indecencies
15	individual	no
16	individual	Social determination of privacy individual decisions
17	-	-
18	individual (youth protection)	no
19	ambiguous	decencies
20	individual (youth protection)	no
21	individual	no
22	individual (youth protection)	no
23	individual (youth protection)	no
24	individual	no
25	individual (youth protection)	Privacy relies on the acceptance of others

26	individual	no
27	individual	no
28	individual (youth protection)	no
29	ambiguous	-
30	ambiguous	-

Table 6: Notions of privacy: Who defines privacy?

Beside the context of SNS, we partly found in our interviewees' general reflections about the meaning of privacy aspects that point to a more inter-subjective or societal notion of privacy. For instance, interviewee 2 and interviewee 6 argue that people's notion of privacy is culturally determined. Additionally interviewee 6 recommends a social privacy notion that is grounded in individual privacy needs. S/he argues:

„As a lawmaker, one probably has to average out people's privacy claims and needs, and then this result should be protected."

Interviewee 16 argues that individual privacy needs are nurtured by society: "For me from a political point of view it is problematic if one declares very much things private and if one believes that this is an individual thing but in fact it is something societally nurtured."

Interviewee 25 provides an informative approach to define privacy inter-subjectively. S/he argues: "In my perspective privacy means that my attitudes and thoughts are respected by others."

Interviewee 8 describes a privacy relevant situation from her/his life and reports the following: "There was an incisive, rather sad, event and after it a lot of people wanted to talk with me about it. But I didn't want it and they have accepted it. It was respected that this is my privacy [...]."

Both interviewees stress that the social recognition of privacy is an aspect of privacy itself. This is similar to privacy theories, put forward by social psychologists. For instance, Barry Schwartz (1968) provides a dialectic understanding of privacy. He argues: "Rules governing privacy, then, if accepted by all parties, constitute a common bond providing for periodic suspensions of interaction." (Schwartz 1968, 742) Here it becomes apparent, that the private of the individual is not possible without social interactions. Schwartz and also Altman (1979, 9) develop an understanding of privacy that is based on the dialectical social theory of Georg Simmel. An interesting aspect of these approaches is that an ideal situation of privacy where subjectively and societally desired privacy can come to accordance.

Interviewee 4 provides a very interesting argument in context of societal privacy notions and how to reach an accordance of individual and societal privacy needs potentially. S/he argues that increased social equality would also increase the freedom to keep things private:

"I think, the more a rule is valid for all society members the more privacy can be granted to the individual. If everybody would disclose his or her date of birth, name,

size, and eye colour then this would be perfect because all know this. The four points and the rest are individual. But if only 50% have to disclose this and the other 50% this and also three points on top, then I probably would plead for more data that is public accessible. This situation is about a relation of disparity. The more uniform it is the less one should have to disclose, I think."

How can interviewees' answers to our three questions (Why do SNS users value or do not value? What aspects of life, do they think are private, which limits to privacy do they see? Who defines what privacy is? Is it up to the individual or is privacy intersubjectively defined by society?) be related to theoretical discussions about privacy and our hypotheses?

Within the privacy literature there is a debate about the status of the privacy value. Is privacy an independent value or can it be reduced to other values. Additionally among scholars who assume that privacy has independent value, which is the majority, there is also a debate how the value of privacy can be justified. Is privacy possible to justify extrinsically, that is only in recourse to other values, such as freedom and autonomy, or has privacy an intrinsic, standing on its own value? In practice however this debate itself is of less value as it is hard to differentiate between both justificatory ways and both ways do not strictly contradict each other; hence a value standing on its own can be justified on behalf of other (intrinsic) values (Rössler 2001, 130-131; Fried 1970, 140; Solove 2009, 84).

The results of our study support this approach towards the value of privacy. Privacy is a crucial, non-reducible value, but it is neither clearly intrinsic nor extrinsic from the following reasons:

On the one hand, we found that most interviewees use other values, such as freedom and intimacy, to express why privacy is important. This would support that privacy is an extrinsic value.

Concerning the line of argumentation revolving around withdrawal, silence, regeneration, concentration, protection, time for (self-)reflection and thinking, and relief, one can either argue that these references are instances of an intrinsic value of privacy or the same references can be interpreted as a recourse to other values. The latter would also support that privacy is an extrinsic value.

On the other hand, one results of our research is that it is obviously hard to answer the question why they value privacy for most of our interviewees. Often it needs several probing efforts to receive an answer to this question and within this process interviewees often argue that it is "just a feeling for no reason" (Interviewee 26) why they value privacy. This would support that privacy is an intrinsic value.

In respect to control and access theories of privacy, we found, contrary to our initial assumption that a trans-subjective notion of privacy is not necessarily linked to access theories; rather it is only one opportunity within this strand of theories. This

modification became clear during our analysis of the interviews: Interviewee 21 holds a typical privacy notion that is based on the control theory:

> *You lose privacy, "if you don't control and cannot ensure that information flows where you want it to flow respectively if only the person who you have chosen will receive the information."*

The control theory allows decision to what extent information should flow and towards whom information should be private. Interviewee 21 focuses here on the subjective and formal dimensions of privacy solely. This is different with interviewee 13, for instance. S/he specifies what privacy is:

> *"Privacy is, for me, something [that I have] when I am at home and I have my own four walls. That is my privacy. That is my home where I have my relatives or friends who I share my life with. I do not share it with all the others but only with a circle that I choose more or less."*

S/he focuses on the subjective dimension of privacy ("for me" and "I choose") but makes substantial claims what privacy actually is ("relatives or friends"). Contrary, interviewee 19 points to a trans-subjective definition (privacy for all) that is about physical distance and the body:

> *"What I want to say is that it is a cultural question […]. It is just not proper that another person invades one's self determined space […]. At first, it is impolite. I have nothing to hide, but I am bothered when somebody comes through this protective wall around me, protective wall may be the wrong term … when somebody enters this defined space around me. […] In Italy, where I stay from time to time, everybody stands so close that and nearly spits in your face. In Sweden everybody would keep 2 metres distance and shouting at each other."*

To decide between control and access theory of privacy involves in our view a twofold; the aspect of who defines privacy and the aspect of what privacy is (its content). It is imaginable to apply the access theory strictly individualistically: A certain realm is private, just for me; others may define different realms. The answer to the question who defines what privacy is not necessarily included within the access theory of privacy. One can argue that both, interviewee 13 and interviewee 19 hold an access theory of privacy, but only interviewee 19 combines this with a trans-subjective approach to privacy.

Whereas a notion of privacy, understood as a private realm and restricted access to it, is open to social and collective negotiations about which realms should be private for all, the control theory of privacy remains strictly individualistic because it deals in fact with formal "freedom to chose privacy" (Wacks, 2010, 41). Therefore one can criticize these theories as subjective formalism: "It is, in other words, a definition which presupposes the value of privacy" (Wacks 2010, 41). Self-determination over personal information requires no other social commitment than the commitment that it should be up to the single individual to decide what privacy is (however this commitment is often not recognised as a social commitment). The control notion of priva-

cy fits best into overall societal tendencies of individualism in Austria and other capitalist societies (Campbell and Carlson 2002, 583). But also individualistic access notions of privacy are in accordance with the extreme relevance that is attributed to the individual, its responsibility, and its decision-making ability in our (individualistic) societies. Not surprisingly, subjective privacy definition, in particular in the form of formal control of information is the grounding notion of almost all conducted empirical research (Sevignani 2011; Fuchs 2009, 11-22; see also Fuchs 2010; 2011a) and it is the dominant privacy notion that we have found among our interviewees.

Given the fact that most of our interviewees not only hold an individualistic notion of privacy but also define private realms, we assume that pure control theories do not explain the meaning of privacy for our interviewees appropriately. We are therefore not able support the hypothesis that users typically have privacy notions that are based on the control theory; rather we found that interviewees typically have individualistic notions of privacy. Aside pure control and access theories of privacy, attempts to integrate as well the subjective control aspect as the access aspect within one theory (see e.g. Tavani 2008, 144-146; Nissenbaum 2010) reflect privacy notions in our sample more appropriately. The same approaches also try to overcome the individualistic bias of control theories (introducing for instance trans-subjective categories, such as "context"; see Nissenbaum 2010). This goal however contradicts the dominant individualistic privacy notions that we have found in our sample. We conclude that it is not sufficient to construct advanced, non-biased theories of privacy; we also need to explain why people hold individualistically biased privacy notions to large extends. What are their material foundations and how can we change them when we want to overcome biased notions of privacy?

For our study we are able to conclude in this context:

- It is crucial to overcome pure control theories of privacy in research by recognising that there is certain content deemed private by SNS users.
- Politically, various and probably dissenting individual notions of the content of privacy should be taken as a starting point for a trans-subjective negotiation process about a common notion of privacy. Within this democratic process dissenting privacy interests probably cannot be overcome completely, but there is a chance to overcome individualistic notions of privacy when people recognise that individual privacy opportunities are not necessarily opposed to societal interests in privacy. The fact that interviewees see limitations to privacy oriented on the common good can be interpreted as a suggestion to think about trans-subjective definitions of privacy. Societal negotiations about what privacy is, should consequently respect those things that they do not want to see private. Based on our empirical results a trans-subjective notion of privacy could include the following:
- Privacy is always based on the respect of others; it is therefore a categorical mistake to see the issue purely individualistically.
- Equality among people could strengthen the real opportunities to privacy that people have. Privacy for whom, is a crucial question in this context. Corporati-

ons and organisations should not have the right to privacy. Furthermore the exploitation of privacy through targeted advertising and the trading of privacy should come into focus (see 4.3).

- Mandatory privacy protection could be extended beyond youth protection. According to targeted advertising on SNS this would mean that society passes a law that regulates that targeted advertising can only be implemented in the form of opt-in and that opt-out versions are considered as violations of privacy and legal breaches of data protection regulations. Such legal provision limits company's behaviour and thereby creates a certain protective sphere for users. At the same time, it enables certain user behaviours within this sphere, namely the individual selection which personal data should be made available for the purpose of targeted advertising.

4.3. Attitudes towards advertising on SNS

The particular focus of the study at hand is the surveillance based business model of commercial SNS, which is advertising. In this case we clearly can speak of surveillance that includes power inequalities: The SNS provider owns the means of surveillance and can set the environment within surveillance takes place. We explore SNS users' attitudes towards advertising on SNS and whether they think that advertising is a problematic form of surveillance or a privacy invasion. What applies to economic surveillance in general applies to economic surveillance for advertising purposes on SNS in particular. Economic surveillance for advertising purposes on SNS nearly completely lacks empirical research.

Interestingly and unexpected 8 of 22 interviewees, who linked the economic aspect to the term of surveillance, named advertising as a form of economic surveillance. Obviously advertising – to a certain extend and for certain users – is visible as a form of surveillance. We therefore cannot explain attitudes towards advertising on SNS by referring to users (lack of) awareness of this issue. Visibility is obviously a much broader category. Hence we should also take into account the knowledge of advertising, which includes more than the awareness that it exists and the visibility of consequences as relevant predictors of attitudes towards advertising.

In order to clarify awareness and knowledge of targeted advertising, we asked interviewees for their awareness of the SNS' terms of use and privacy policies (IQ17 and 18), tried to assess their knowledge how advertising works on SNS (e.g. that it is targeted) (IQ22, 23, 25, and 26), and whether they think that advertising influences the appearance or functionality of the SNS (IQ24). 9 Interviewees have a fairly high awareness of the SNS' terms of use and privacy, which means that they have read the documents at least partly and witnessed changes of them. About 17 interviewees can be said that they have a fairly low awareness of the documents because they have at least witnessed changes in the documents but have not read them. 4 interviewees have no awareness at all of the documents; they have neither witnessed changes nor have read the documents. We can conclude that the majority of SNS users in our sample have low or no awareness of the terms of use and privacy policies. Also about those with a fairly high awareness, cannot be said that they are experts who are able

to provide information about what exactly the SNS provider is allowed to do: Their awareness is only high in relation to the average of the sample.

We found that the majority of our interviewees (18 out of 30) have a medium knowledge of how advertising works on SNS. These interviewees know that advertising on SNS is personalised or targeted but do not know more about how targeting works or hold wrong assumption about it. Only 2 interviewees have a high knowledge about this issue; they were able to provide correct descriptions how personalised or targeted advertising works on SNS (he or she may hold some additional wrong assumptions about it). 5 interviewed users have a low knowledge, they know that there is advertising on SNS but do not know more about it. At least 5 interviewees are not aware that advertising exists on SNS at all. We can conclude that for one third of our sample the advertising business model of SNS that is based on user surveillance is not much visible.

On the other hand, we also asked our interviewees whether they think that advertising influences the appearance or the functionalities of SNS at least in a way. The majority of the interviewees (18 out of 30) think that it does so. Only 7 users state that advertising does not influence the SNS.

case	Awareness of the terms of use and privacy policy	Degree of knowledge about how advertising works	Perceived influence of advertising on SNS
1	High	Medium	influences SNS
2	No	no	-
3	Low	low	does not influence SNS
4	High	medium	does not influence SNS
5	Low	low	influences SNS
6	High	medium	does not influence SNS
7	Low	high	influences SNS
8	Low	medium	does not influence SNS
9	No	no	does not influence SNS
10	Low	Medium	-
11	Low	high	influences SNS
12	No	No	-
13	Low	Medium	influences SNS
14	Low	no	influences SNS
15	Low	Medium	influences SNS
16	Low	Medium	influences SNS
17	High	Medium	influences SNS
18	Low	Medium	-
19	High	Medium	-
20	No	Medium	influences SNS
21	High	Medium	influences SNS
22	Low	Medium	influences SNS
23	Low	no	does not influence SNS
24	High	Medium	influences SNS
25	Low	low	influences SNS
26	Low	low	does not influence SNS
27	High	Medium	influences SNS
28	High	low	influences SNS
29	Low	Medium	influences SNS
30	Low	Medium	influences SNS

Table 7: Visibility of advertising on SNS

Interviewees associate employer surveillance just as often as they associate advertising with the term surveillance. 13 interviewees are critical of employer surveillance (does worry and/or do not like it) and 10 interviewees disagree with targeted advertising before we gave our information input. Hence we were not able to detect significant differences in users' overall awareness and their attitudes towards these two forms of economic surveillance.

Whereas awareness and knowledge of (targeted) advertising was explored on behalf of separate interview questions, we found the other aspect of visibility, namely the visible consequences of advertising, manifest in interviewees' attitudes towards advertising on SNS. Within the responses to IQ23, 27 and then 28, 29, 30, and 31 we were able to identify three influential lines of argumentation belonging to a positive attitude towards advertising on SNS (in total with 13 interviewees): First and most ofthen, interviewees say, that advertising and advertisements show no negative consequences for them because they are not forced to notice advertisements, to click on them, and to buy advertised products ultimately. Moreover, they are not forced to participate in SNS too. For instance interviewee 20 says:

"I don't care, either I buy it [advertised product] or not. No problem, they can show it to me, one should be strong enough to resist."

Second, interviewees made clear that advertisements on SNS show positive consequences for them, such as that they provide useful product information and interesting offers, and that it is fun watching them. The most important positive consequence indentified by the interviewees, however, was that advertising makes the usage of SNS free for them. For instance interviewee 8 says about advertising:

"Partly it is useful. When I see certain special offer then I can buy them; that can be useful too." And interviewee 12 argues that advertising is "in principle no bad thing. We get our student party that we organise one a year also financed by advertising. Therefore I find it totally OK. One hand washes the other!"

Third, Interviewees also agree with advertising on SNS as they find it a common and societal recognised funding model and because we all are used to have it. For instance, interviewee 14 was asked what her/his opinion about advertisements is, and s/he answered:

"Well, it is important for competition [...]" and she further explains: "If nobody knows the products then nobody will buy them". Interviewee 15 assists: "It is obvious that they have to get financed, and if anyone is annoyed then he or she is not forced to register". Similarly, interviewee 19: "at the first, it is my private pleasure to log in, I have the opportunity to not using it - at least from a legal perspective. It is then a matter of dispute which consequences I will face, when I opt out from a medium that is used by all. But within the frame of terms of use and privacy settings, which you agree with without reading, it is Ok from a legal perspective [...]. For me it is no big deal. Within a market society, I think, it is a legitimate desire that

the supply side explores the demand side. As long as it happens within law or private contract, it is OK."

Interviewee 20 balances advertising funding against alternative funding models that s/he finds not that established and well-recognised:

"Honestly, it is way better that they earn money on behalf of my data and do in turn nothing stupid with it than they are financed by donations, run out of money and therefore try to make profit from my data illegally. Better they do adverts for Zalando [a highly advertised online shop] and Zalando finances the SNS for me and nothing else happens [to my data]"

case	Attitudes towards advertising on SNS (applied arguments)	Attitudes towards advertising on SNS as a problematic form of surveillance or privacy invasion (applied arguments)
1	Disagreement (no other choice; negative consequences)	Ambiguous (no negative consequences; Indirect potential negative consequences) [privacy invasion (direct negative consequences)]
2	Disagreement (no other choice; negative consequences)	No privacy invasion (informed consent; no negative consequences) [privacy invasion (indirect potential negative consequences)]
3	Disagreement (contradicts SNS's goal)	Privacy invasion (Indirect potential negative consequences; direct negative consequences)
4	Agreement (recognised funding model)	Ambiguous (No informed consent; informed consent) [privacy invasion (direct negative consequences)]
5	Agreement (no negative consequences)	Privacy invasion (no informed consent) [(direct negative consequences)]
6	Ambiguous (no negative consequences; recognised funding model; negative consequences)	No privacy invasion (no negative consequences)
7	Ambiguous (positive consequences; negative consequences)	Privacy invasion (direct negative consequences; no informed consent)
8	Agreement (recognised funding model; positive consequences)	No privacy invasion (informed consent) [privacy invasion (no informed consent)]
9	Disagreement (no other choice; negative consequences)	Ambiguous (no informed consent; no negative consequences) [privacy invasion (direct negative consequences)]
10	Disagreement (no other choice; negative consequences)	Privacy invasion (direct negative consequences; no informed consent)
11	Agreement (positive consequences; no negative consequences; recognised funding model)	Ambiguous (indirect potential negative consequences; direct negative consequences; no informed consent; no negative consequences) [privacy invasion (direct negative consequences; no informed consent)]
12	Agreement (positive consequences; recognised funding model)	No privacy invasion (no negative consequences) [privacy invasion (direct negative consequences; no informed consent)]
13	Agreement (positive consequences; no negative consequences; recognised funding model)	No privacy invasion (no negative consequences) [privacy invasion (no informed consent)]
14	Ambiguous (recognised funding model; no positive consequences) [Disagreement (negative consequences)]	Privacy invasion (direct negative consequences) [(indirect potential negative consequences; no informed consent)]
15	Agreement (positive consequences; no negative consequences)	No privacy invasion (no negative consequences)
16	disagreement (Contradicts SNS's goal)	No privacy invasion (no negative consequences) [privacy invasion (no informed consent)]
17	disagreement (negative consequences)	No privacy invasion (no negative consequences)
18	Ambiguous (negative consequences; positive consequences)	No privacy invasion (no negative consequences) [privacy invasion (direct negative consequences)]
19	agreement (recognised funding model; no negative consequences)	No privacy invasion (no negative consequences) [privacy invasion (direct negative consequences)]
20	agreement (recognised funding model; no negative consequences; positive consequences)	No privacy invasion (no negative consequences) [privacy invasion (indirect potential negative consequences)]
21	Disagreement (contradicts SNS's goal; negative consequences)	Privacy invasion (direct negative consequences; no informed consent) [no privacy invasion (no negative consequences)]
22	Ambiguous (recognised funding model; no negative consequences; negative consequences)	No privacy invasion (no negative consequences)
23	Disagreement (negative consequences)	Privacy invasion (direct negative consequences; no informed consent)
24	ambiguous (positive consequences; negative consequences)	Privacy invasion (direct negative consequences; no informed consent)
25	Agreement (positive consequences)	No privacy invasion (informed consent; no negative consequences) [privacy invasion (no informed consent; direct negative consequences)]
26	Agreement (positive consequences; no negative consequences)	No privacy invasion (no negative consequences) [privacy invasion (no informed consent; direct negative consequences)]
27	Ambiguous (positive consequences; negative consequences)	Privacy invasion (direct negative consequences)

28	Agreement (positive consequences)	Privacy invasion (direct negative consequences; no informed consent)
29	Agreement (positive consequences; no negative consequences)	No privacy invasion (no negative consequences) [privacy invasion (no informed consent; direct negative consequences)]
30	Disagreement (negative consequences)	Privacy invasion (indirect potential negative consequences; direct negative consequences; no informed consent)

Table 8: Distribution of arguments regarding attitudes towards advertising on SNS and regarding attitudes towards advertising on SNS as a problematic form of surveillance or privacy invasion [including changes in attitudes after information input]

On the other hand, we were able to discern four strands of arguments opposing advertising on SNS (in total with 10 interviewees). The first and the second are diametrical opposed to the first two positive strands. First, interviewees pointed to negative consequences of advertising for them. A particular strong expression of this strand is the argument that advertising on SNS is pressing, manipulating, and creates (unwanted) new needs. This is expressed in the following passage from interview 17:

"There is always the illusion that advertisements would not influence people, and so people unfortunately participate voluntarily. They think that they have a free will about what they like and hence that they are not influenced by advertisements. But, of course that is wrong [...] because needs that you have are inhered to a small extent only. The most of what we consume is [related to] culturally acquired needs. [...] Precisely because in advertisements products are linked to emotions or opportunities of self-expression [...], the most of the needs rise ... apart from food". And interviewee 1 specifies: "The problem thereby [with targeted advertising] is that needs are created in a very efficient way because one is confronted with exactly the advertisements one is prone to".

The most frequent negative consequences interviewees pointed to, are however weaker than manipulation and include annoyance and deflection. Interviewee 23 argues accordingly:

"One is no more able to choose and to filter as adverts are everywhere [...]. That is tremendously annoying. It annoys me most if additional windows pop up and one have to close them first before one is able to proceed. I feel that is going even worse. It used to be not that bad, but now, of course, it is made use of it."

Second, interviewees frequently argue that advertising shows no positive consequences for them and that it is unnecessary and a waste of time. This argument is still weaker and fairly applied. Third, interviewees argue that advertising contradicts SNS's inherent and real goal that is about maintaining and establishing social relations. Hence SNS should not be about advertising for profit purposes. Interviewee 16 states:

"My claim to a SNS is that it is a SOCIAL network, and that it provides me with the opportunity to organise and exchange with others etc. That is what matters for a SNS and advertising is no necessity for a social network. That is a feature which is necessary for a company [...]."

In this context, interviewees also expressed their fear or actual observation that advertising determines or influences SNS's content and structure. Fourth, interviewees lament that there is no alternative to this funding model (see below). Here, the identified arguments were similar to the third positive strand of argumentation, but interviewees turned the arguments negatively instead of being affirmative. Interviewee 1, for instance, argues that advertising is "a necessary bad" and interviewee 10 explains this:

"I think there is no alternative choice. I think it is not OK [...] I bother that my data is sold for economic purposes, that someone is making profit with it and I do not agree with that./ Interviewer: One could argue that you have already agreed when you agreed with the terms of use in the beginning.../ I have the decision to exclude myself or to agree to be in. I have to decide, there is nothing in between."

During the interview process we found that 7 interviewees make usage of software tools that hide advertisements in the Internet browser. Ad-blocker software does not prevent the collection of personal data; it only prevents the display of advertisements to the user. Not surprisingly, we found that those who use ad-blocker software at the same time think that advertising influences the appearance and/or functionalities of SNS.

	Make use of ad-blocker software	Do not make use of ad-blocker software
Advertising influences the SNS	5	13
Advertising does not influence the SNS	0	7
No information	2	3

Table 9: Relation between the use of ad-blocker software and perceived influence of advertising on SNS

One can assume that those who make usage of such software do not agree with advertisements on SNS. Indeed we found that most of them disagree with advertising on SNS or have ambiguous attitudes towards this issue.

	Make use of ad-blocker software	Do not make use of ad-blocker software
Agreement with advertising on SNS	1	12
Disagreement with advertising on SNS	3	7
Ambiguous attitude	3	4

Table 10: Relation between the use of ad-blocker software and attitudes towards advertising on SNS

Interviewee 11 makes use of ad-blocker software but agrees with advertising in general. S/he argues:

"In principle, I think advertising is legitimate. It is an element of our system, one has to get financed. If I run a site then I have to finance servers and employees. It is completely OK to do advertising. As I said before, it annoys me with Facebook, but

in general it is OK./ Interviewer: Why is it annoying with Facebook?/ On the one hand, it is difficult to differentiate between content and adverts on Facebook. And on the other hand, [...] I'm not keen on facing ads all the time that deflect my attention. [...] They earn enough money, so they don't need my clicks on top."

Interviewee 11 concludes it is not reprehensible to do targeted advertising but s/he argues "in the end, I don't care" as s/he uses ad-blocker software that s/he can selectively switch on and off according his/her preferences. Interviewee 11 reports that s/he disables the ad-blocker software on other websites than Facebook. It is the specific SNS Facebook that s/he does not want to support with clicks on adverts. Interviewee 11 shows contradictory attitudes: He welcomes the SNS Facebook and its funding through advertising, but does not want to contribute to it.

In order to find out which role surveillance and privacy plays in shaping interviewees' attitudes towards targeted advertising, we asked them whether or not they perceive advertising on SNS as a problematic form of surveillance or a privacy invasion. Again, the distribution is nearly balanced, but the number of interviewees holding an ambiguous attitude towards this question is less high. Obviously, the question is more easy to answer decisively (15 Interviewees said that it is not problematic and not affecting their privacy invasively, 11 said that it is a privacy invasion or a problematic form of surveillance, 4 remain ambiguously).

Arguments neglecting advertising as a problematic form of surveillance or a privacy invasion could be easily and clearly grouped into two major strands of argumentation: First, it was argued that there was an informed consent by the user to the SNS's terms of use, which also includes the acceptance of targeted advertising. Therefore it is principally accessible for everyone how advertising works on SNS. The importance of an informed consent to advertising, which is also referred to by users that see advertising as a privacy invasion, is expressed by interviewee 2:

"(...) they have to have knowledge about what they can choose. Usually during or before the registration, there should be a detailed description what user can do, what they can enable, and what they can keep private and what they cannot keep private. Once I have registered then it is too late for that. Of course, one can unsubscribe. However, it is crucial that I have the information about to what extent I will be able to protect my privacy in advance."

Second, similarly to one strand of agreement listed above, it was pointed out that advertising on SNS shows no negative consequences for users. The particular argument in this context is that one cannot be identified by third parties (any actor outside the relationship between user and SNS provider). Here, interviewees adopt the line of argumentation which is offered by the SNS provider in their terms of use and privacy settings. For instance, interviewee 22 argues:

"Well, it is in it [the terms of use]; it is not really related to the person. Therefore, it is no big deal because it [collected data] is not connected to my name. [...] As long as

it is not related to the person, it is OK, once my name is added, it is not". Similarly, interviewee 18: "That is not a problem for my. I think advertisers need statistics, otherwise it would not work. This is not a tragedy, if it is not associated with my person."

Interviewees, who think that advertising on SNS is a problematic form of surveillance or a privacy invasion, employed the following strands of arguments (here again in parts, arguments oppose to the neglecting ones diametrically). First, interviewees challenge that there was an informed consent to advertising. They think that it is not obvious that privacy settings do not apply for advertising and the SNS provider is allowed to use "private"-marked information for its purposes. This cannot be understood from the SNS's terms of use as they are confusing and unclear. Interviewee 5 is a good example, s/he argues from the beginning that the usage of personal data for advertising purposes is problematic as it:

"is something that nobody knows explicitly. Again there happens something that I'm not aware of and to which neither consent nor I'm able to reject it. It just happens."

Contrary to the positive arguments, interviewees also argued that advertising is problematic because it shows negative effects. In this context, interviewees differentiated between direct, indirect, and potential consequences for their privacy. Interviewees secondly argued (referring to direct consequences) that advertising on SNS is a problematic form of surveillance as it is too excessively and disproportionally performed by the SNS provider. This applies in particular when surveillance is performed on other sites than the genuine SNS. Interviewee 21 expresses this:

"As I said, this bears no proportion. The whole system, how Facebook is financed and works, makes it understandable form their perspective that they need certain information and process them. However that does not justify the multitude of data [that is collected] because, in my view, an incredible portion of it is not needed at all."

It is also argued that the SNS provider itself invades users' privacy. Interviewee 23 explains this:

"That is a kind of distortion. They say that they pass it away anonymously, but it comes back to me [...]. When it comes back to me with the advertisement that is targeted to me, then that is not anonymous." Similarly, interviewee 30: "Nevertheless I am bothered by advertisements and the feeling is conveyed as if they know all about me."

These various arguments show that interviewees see direct consequences for them and therefore see advertising on SNS as a problematic form of surveillance or privacy invasion. Third, interviewees argue, that advertising on SNS shows indirect consequences because the data collected for this purpose can be accessed by third parties,

such as state authorities or hackers, later on. An example for these fears is interviewee 1:

> *"Surely it is something different, the advertising companies receives not my name but only a anonymous person that has a certain user behaviour, profile, or interest [...]. It becomes quite questionable when it [the data pool] is somehow cracked and this is surely possible, I think. Well, the data come from this site somehow. Therefore there is only a theoretical protection but a hacker has surely the skill to relate the data to the person."*

Fourth, interviewees are uncertain about the exact use of their data and this uncertainty is linked to potential consequences for them. In this context they are also afraid that SNS will collect and use ever and ever more data in the future. Uncertainty and potential consequences together are perceived as privacy-invasive. In the following passage from interview 3, dealing with the SNS provider's point of view that there is a separation between privacy issues and advertising, this is expressed:

> *"That is exactly the point [when it comes to targeted advertising], where I would say that it starts becoming uncontrollable because you are no more able to understand what happens in the background. You have this surface, where you can change things, but that what is behind is not under my control, although it affects my privacy."*

Within a societal climate of consumerism (Jhally 1990; Haug 1986; 2006) advertising is frequently perceived as an ordinary process and as harmless, at best a bit annoying, or – especially in its targeted form – it is even desired by the users in order to receive suitable offers to satisfy their needs. Once users are well informed about the linkage between commercial character and its dependence to watch the users for business purpose (Fuchs 2010, 181), and once they are aware of potential alternatives of funding SNS, we then hypothesize that SNS' users typically argue that they see targeted advertising as a privacy threat and as a problematic form of surveillance (Fuchs 2011b, 142-145; hypothesis 3a). A survey conducted by Turow et al. (2009) supports our assumption: "Contrary to what many marketers claim, most adult Americans (66%) do not want marketers to tailor advertisements to their interests. Moreover, when Americans are informed of three common ways that marketers gather data about people in order to tailor ads, even higher percentages - between 73% and 86% - say they would not want such advertising" (Turow et al. 2009, 1). We found that most of our interviewee have no or low awareness of the SNS' terms of use and privacy policies and have low or medium knowledge about advertising on SNS. Therefore, as part of our participatory research approach, we confronted the interviewees with information about how advertising on SNS works, that it is targeted and demands a wide range of various personal data categories to perform (see the handout as part of our interview guide). Then we ask them, now having in mind the provided information, again what their attitudes towards advertising are. In accordance with

others, we had the underlying thesis that there is a lack of awareness and knowledge about economic surveillance as it is less visible and shows les direct consequences for the users. Our study supports this assumption, 11 out of 30 interviewees see no negative consequences of advertising for them, and 17 interviewees say that advertising is not a privacy invasion because it shows no negative consequences for them. The idea was to receive a more accurate image about users' attitudes towards advertising once they are informed about how exactly advertising and surveillance work on SNS.

After the information input, we indeed could observe a significant number of interviewees who switched to a negative perception of advertising. They see it now as a problematic form of surveillance or a privacy invasion, or, in two cases, as they have already perceived it as a privacy invasion they switched from agreement to disagreement with advertising on SNS. In one case the direction was however reversed. Interviewee 21 previously thought that advertising on SNS is a privacy invasion thinks now that it is not a privacy invasion. S/he has thought that personal identified data are handed over to advertisers and has not known that it is processed anonymously. Once they knew that data is processed anonymously for advertising purposes, s/he argued that it is not a privacy invasion.

Beside that case, there were 13 interviewees who previously stated that advertising on SNS is neither a problematic form of surveillance nor a privacy threat, or have had an ambiguous attitude, but were later changing their opinion. The most influential argument in these swing cases was that the data collection goes too far. In particular, it was argued that some of the collected data (for instance data collected on other websites) have nothing to do with the SNS, and that this was not obvious to the interviewees, and that they have not given an informed consent to this.

In the context of the disproportion argument, interviewee 18 makes an interesting analogy between the online and the offline world:

> *"For instance I think the thing about the other sites that I have visited is a privacy threat. I know about the thing I do on Facebook that they cannot be entirely private. But things are different with other web-sites; I assume that I close one door and open the next one. That is of course a privacy issue."*

An interesting question is to identify whether awareness and knowledge of advertising on SNS determines interviewees attitudes. Generally no obvious regularities between awareness of the terms of use and privacy policies, as wells as the degree of knowledge about advertising on the one hand, and specific attitudes towards advertising on SNS exist, on the other hand. For instance, we found no support for the assumption that low visibility, as it was indicated by the interviewees, resulted in agreement to advertising on SNS or in the likelihood that interviewees think about advertising as no privacy issue.

Only those who have no awareness of the terms of use and privacy policies tend to change their attitudes once they got the information input by our side. On the other

hand, those who have high awareness of the terms of use and privacy policies tend to stick with their previous attitude.

	High awareness	Low awareness	No awareness
No changes	7	8	1
Was privacy invasion; is now no privacy invasion	1	0	0
Was ambiguous; is now privacy invasion	0	0	0
Was no privacy invasion; is now a privacy invasion	1	9	3

Table 11: Relation between awareness of the terms of use/ privacy policy and changes of attitudes towards advertising as a privacy invasion/problematic form of surveillance due to our information input

As we deduced the information that we gave out interviewees from Facebook's terms of use and privacy policy, this result is not surprising. Those who had read these documents and/or witnessed changes of them are likely to receive no or not much new information that could bring them to change their attitudes.

The overall significance of changes after the information input let us assume that the degree of users' knowledge and awareness of economic surveillance plays a key role in influencing the perception whether it is problematic or a privacy invasion. Hence the assumption that there is an informed consent becomes quite questionable and many users would not agree with advertising on SNS if they knew how it exactly works. After the information input, interviewee 14 replies on the question whether this form of advertising is a privacy invasion:

> *"Actually... it is because I cannot decide whether I want this or not. I also cannot decide to what extent I get oneself into this; rather it is so for no reason. I have decided about all what I publish on Facebook, but when they collect the other sites I have visited only because I am accidently logged in..., well, actually, that has nothing to do with Facebook and they should not be allowed to do that." In the same context, Interviewee 28 argues that "it is no normal advertisement anymore; rather it is an invasion, in particular, when they evaluate whether the advertisement was successful or not. This goes beyond the scope of normal advertisements for financing the site." And interviewee 8 holds the opinion that such surveillance is problematic "because it is something that I do outside of Facebook. I have agreed with the terms on Facebook […] I decide what I publish there and what I do not publish. If I am on another site then it is no longer Facebook, it is not OK that there is a kind of connection. Things I do elsewhere should not of Facebook's business."*

Interesting in this context are the answers of interviewee 16. Before the information input s/he points to the fact that collected data of a person are used for advertising in a statistical, aggregated, and therefore anonymised manner. This is also stressed by Facebook and its argumentation that advertising is not a privacy issue is

grounded in it. After the information input, interviewee changed its attitude and says the following in response to our question whether collecting personal data for advertising is a privacy invasion:

"Generally I have a negative attitude towards advertising; hence I actually have to say 'Yes' In addition with Facebook it is problematic that people are not aware and Facebook does not make it so clear."

Interviewee 16 responded to the probing question after the collection of data on other web-sites than the genuine SNS:

"I'm not surprised but it is of course worse than the other things they do. It is relatively clear that the store what I like; that can easily be seen without reading the privacy policy. But the other things are technical that do not immediately strike the eye. I think that is one thing that they have done for companies."

Beside the already known arguments that data collection goes too far and one cannot assume a informed consent to it, another point is of interest here: Interviewee 16 stresses that s/he "actually have to say 'Yes'", it is a privacy invasion but argued before that the anonymity of data collection contradicts a privacy invasion. We can interpret this as an evidence of the influence of the privacy discourse in order to oppose to Facebook. Disagreement with advertising, which is the attitude of interviewee 16, tends to be expressed on behalf of the privacy discourse.

case	Attitudes towards advertising	Attitudes towards privacy and advertising	Changed attitudes towards advertising after information input	Changed attitudes towards privacy and advertising after information input	Use of ad-blocker software
1	Disagreement	Ambiguous	No changes	Privacy invasion	No
2	Disagreement	No privacy invasion	No changes	Privacy invasion	yes
3	Disagreement	Privacy invasion	No changes	No changes	No
4	Agreement	Ambiguous	No changes	No changes	No
5	Agreement	Privacy invasion	No changes	No changes	No
6	Ambiguous	No privacy invasion	No changes	No changes	No
7	Ambiguous	Privacy invasion	No changes	No changes	Yes
8	Agreement	No privacy invasion	No changes	Privacy invasion	No
9	Disagreement	Ambiguous	No changes	Privacy invasion	No
10	Disagreement	Privacy invasion	No changes	No changes	No
11	Agreement	Ambiguous	No changes	Privacy invasion	Yes
12	Agreement	No privacy invasion	No changes	No changes	No
13	Agreement	No privacy invasion	No changes	Privacy invasion	No
14	Ambiguous	Privacy invasion	Disagreement	No changes	No
15	Agreement	No privacy invasion	No changes	Privacy invasion	No
16	Disagreement	No privacy invasion	No changes	Privacy invasion	Yes
17	Disagreement	No privacy invasion	No changes	No changes	No
18	Ambiguous	No privacy invasion	No changes	Privacy invasion	Yes
19	Agreement	No privacy invasion	No changes	No changes	No
20	Agreement	No privacy invasion	No changes	Privacy invasion	No
21	Disagreement	Privacy invasion	No changes	No privacy invasion	No
22	Ambiguous	No privacy invasion	No changes	No changes	Yes
23	Disagreement	Privacy invasion	No changes	No changes	No
24	Ambiguous	Privacy invasion	No changes	No changes	No
25	Agreement	No privacy invasion	No changes	Privacy invasion	No
26	Agreement	No privacy invasion	No changes	Privacy invasion	No
27	Ambiguous	Privacy invasion	No changes	No changes	No
28	Agreement	Privacy invasion	disagreement	No changes	No
29	Agreement	No privacy invasion	No changes	Privacy invasion	No

30	Disagreement	Privacy invasion	No changes	No changes	yes

Table 12: Attitudes towards advertising on SNSs, Attitudes towards advertising on SNSs as a privacy invasion or a problematic form of surveillance, Changes of attitudes towards advertising and advertising as a privacy invasion or problematic form of surveillance because of information input during the interview, and use of ad-blocker software

Among two interviewees we found an untypical constellation; they agree with advertising on SNS but see it at the same time as a problematic form of surveillance/privacy invasion. Whereas it is immediately understandable when interviewees disagree with advertising on SNS but do it from other reasons than thinking that it is a privacy invasion. Interviewee 5 and 28 seem to be contradictory here. They also do not change their attitudes after the information input. It is notable that both interviewees have low knowledge how advertising works on SNS, that it is targeted for instance. Interviewee 5, for instance, agrees with advertising because:

"it is up to me whether I click on it or not."

S/he assumed that it is possible for users to determine if and what data can be used for advertising purposes and only her clicks on advertisements can be used for further advertising. S/he was surprised that Facebook has the right to use the data for advertising without any special permit beside the agreement to the terms of use and privacy policy. S/he overestimates the power of the user in this regard due to a lack of knowledge and therefore the contradictory constellation becomes understandable. Things are similar with the second case, interviewee 28. S/he assumed that there is traditional banner advertisement on SNS and not targeted advertising that involves the usage of personal data. Also here the lack of knowledge helps to explain the contradictory constellation.

4.4. User exploitation and privacy as commodity

According to our critical theoretical background, advertising on SNS relates to user exploitation. IQ30 and 33 from our interview guide were strongly influenced by our theoretical framework and helped to explore the issue of exploitation on SNS. Do users think that they are exploited while using SNS? This question exposes us to a certain problem that we are facing when we use a Marxian notion of exploitation. Mark Andrejevic has pointed to this problem: "Exploitation is also not definable solely in terms of subjective sensibility: it is not reducible to whether or not individuals feel they are the victims of exploitation. Such feelings may indeed be accurate, and yet they do not define exploitation. That is to say, exploitation may exist in the absence of a subjective sense of victimization" (2011, 91). In this context, our methodological premise becomes crucial that SNS users are not only informants to us and exploited, but also partly having wrong or skewed sense about societal power and domination structures. We have to be aware that interviewees tend "to reframe structural condition as questions of individual pleasure and desire" (Andrejevic 2002, 283) and therefore do not feel exploited.

We assume that one aspect of feeling exploited is that users are kind of aware that people who own and control the SNS are appropriating societal produced surplus, and that interviewees therefore want compensation in return. According to our theoretical framework "nobody is unproductive since each human being is producing and reproducing the commons appropriated by capital" and "capital should in return give something back to society" (Fuchs 2010, 193).

Among our interviewees, only 9 users stated that they want compensation, the majority of 17 users do not want compensation, and 4 users have an ambiguous attitude towards this question. We mainly identified one influential line of argumentation among those who want compensation: Interviewees see a bad or exploitative ratio between the SNS's profits and their own benefits of using the SNS. Interviewee 12 expresses this clearly:

> *"Facebook is earning so much money; therefore it is my opinion that one should receive something extra to using the site for free."*

Marxists, when criticising exploitation, criticise not only the extend of exploitation but also its precondition, i.e. the right to have others work for you, and the private control over the means to realise the work force (which is traditionally the private property in the means of production). To moan a bad ration between SNS' profits and the received advantages is based on a limited understanding of exploitation. Exploitation remains exploitation also when compensation is paid to the user in return. This is because owners of SNS have in mind the surplus when they invest in a project. Would the compensation (embodied in the form of wages or taxes) exhaust the entire surplus, SNS capitalists would not invest and the question of wages or taxes cannot be posed. Interviewee 16, who was included in our sample because we expected that he is quite critical about surveillance and advertising, seems to share this line of argumentation:

> *"I would ask why Facebook should do that, they have no reasons for it. I would maliciously assume that people who call for that [compensation] have a feeling of justice that is not relevant. [...] By the way, I would not think of wage-labour as the way how it can get better. I would not criticise Facebook moralistically, every corporations behaves this way, why should it behave differently".*

However the call for compensation, which we have found among 9 of our interviewees, points to the fact of a feeling of being exploited on SNS exists and also from a Marxist point of view compensation payments are progressive as they support the exploited and would limit the power of capital at the same time. An active political force that wants SNS provider to pay compensation would admittedly not abolish exploitation, but it would, if it succeeded, reduce the exploitation rate and would alter societal power relations between Internet capitalists and the exploited. Given the low number of those who want compensation, it is not surprising that even those who feel exploited have serious doubts about how compensation could be realised politically. They see clearly that compensation payments are contradictory to the common sense

and therefore kind of utopian. They wonder how compensations then can be distributed fairly; but they also mention opportunities to realise compensation payment, for instance they suggest that users should become shareholders/ owners of the SNS. Interestingly, interviewee 24 argues in this context that the argument that compensation payments would ultimately destroy SNS does not hold because there are working alternative examples, such as Wikipedia, that show that Internet services can be sustained without selling personal data.

Interviewees who think that SNS should not pay users any compensation employed the following contrary lines of argumentation: First, instead of pointing to a bad ratio between benefits for them and profits for the SNS, interviewees argue that they have already received compensation, namely in the form of the SNS service that provides them with several advantages and benefits. Second, they argued that the SNS provider behaves completely legitimately. This second strand includes several related arguments: SNS's employees are working for that profit and/ or the SNS's founders had a good idea or good luck, so there is no reason to demand compensation. They think it is the way things simply are and that they do not get money for many other things too. Most importantly, there is also no coercion that forces people to be on SNS, it is my decision to join and to agree with the SNS' terms of use. These two lines of argumentation obviously contradict the critical theories of surveillance, exploitation, alienation, and immaterial labour, and they also do not recognise that there are alternative SNS that work differently.

Among those, who do not want compensation in exchange for the usage of their data, we have found an interesting third line of argumentation (with 4 interviewees). It is interesting because it offers another emancipatory perspective, but has also ideological connotations at the same time. Within this strand, interviewees argue that personal data should not be traded at all and that receiving compensation will not stop this trade; rather any compensation payment is based on such trading. For instance, Interviewee 24 argues that it is not OK to trade personal data:

> *"... because my privacy means a lot to me and I think it cannot be compensated with material goods. Privacy is about my decision and my freedom so that I do not lose my self-control. They should not [be allowed to] exercise so much power over me". Interviewee 9 assists when s/he argues that this would "basically be a form of selling myself" and adds: "Of course, in principle, right now I'm also selling me, however without receiving money in exchange. If one would really receive money then this would perhaps shed more light on the fact that they really take something from you... currently it is not recognisable." Interviewee 25 argues in that context: "I believe such things ... information should not be for sale. [...] In fact, I would then sell my privacy. I wouldn't do that, but maybe there are people that want to made such easy pickings". Interviewee 27 contrast these "easy pickings" with "honestly earned money" that s/he prefers.*

Those interviewees resist the ongoing "reconceptualization of privacy in the consumer's mind from a right or civil liberty to a commodity that can be exchanged for

perceived benefits" (Campbell and Carlson 2002, 588; Comor 2011) (see the section about privacy trade-offs).

Additionally to their claim that privacy should not be for sale, interviewees addressed the issue whether using the SNS, generating data for sale, can be characterised as work. We included the analogy between using SNS and (wage-)labouring intentionally within our question in order to be able to explore this question of immaterial labour. The term, according to Maurizio Lazzarato, mainly refers to two different aspects of ever more relevant forms of labour (132): First, immaterial labour produces "immaterial" content, such as information, culture, or meaning; and, second, the term refers to "immaterial working processes and "involves a series of activities that are not normally recognized as 'work'" (132). Lazzarato mentions several markers that denote the existence of immaterial labour. He argues that, first, the dichotomy between mental and manual labour collapses obviously (133) and that an "integration of scientific labor into industrial and tertiary labor has become one of the principal sources of productivity" (136). Second, nowadays labouring means that the worker has to put its own subjectivity to work, that is all what he actually is, his views, relationship, feelings and so on (133-134): "The 'raw material' of immaterial labor is subjectivity and the 'ideological' environment in which this subjectivity lives and reproduces" (142). Third, he observes that there is a decentralization of production ongoing; labour spreads out of the factory into whole society and its individuals (135). Consequently, fourth, the line between work time and leisure time blurs, in fact "life becomes inseparable from work" (137). And there is also, fifth, a blurring line between consumption and production (137), "consumption is no longer only the 'realization' of a product" (140; see also for this marker in particular Bruns 2008). As Tiziana Terranova notes, immaterial labour is often free labour (2000), and as such "an important, and yet undervalued, force in advanced capitalist societies" (33). She speaks of "free" labour as it is "simultaneously voluntarily given and unwaged, enjoyed and exploited" (36) when it is translated into productive, profit generating activities for corporations. Christian Fuchs (2011a) prefers to speak of knowledge work, instead of immaterial labour. He argues focussing on "immateriality" would support a false presumption that matter and mind are two separated entities. "Nevertheless", Fuchs also finds that the argument, "that social, communicative, and co-operative labour is exploited and transformed into surplus value in exploitation processes, is correct" (2011a, 299). The question of how valorisation and therefore exploitation on SNS can be understood in detail cannot be answered here. Likewise we cannot and but also have not to decide here the question whether immaterial labour has nowadays taken on the general hegemonic role in global capitalist surplus appropriation, as it is stated by several authors (e.g. Hardt and Negri 2004; Pasquinelli 2009; Boutang 2012). However, in order to conclude, we can assess that the combination of surveillance, immaterial labour "is at the heart of capital accumulation on web 2.0" (Fuchs 2011a, 296) and therefore the problems of exploitation and alienation should be a matter of empirical concern.

Besides the above quoted opposition of "easy pickings" and "honestly earned money" (one can add through "real" work), we interestingly found that no interviewee, whether those who want compensation nor those who do not want compensation, supported the analogy between using the SNS and labouring. They applied the following arguments to make clear that using the SNS cannot be characterised as work: Interviewees argue that only the SNS's employees are working, that "the work of being watched" contradicts the common sense how to make money (namely through "real" work), that we use the SNS voluntarily, but work is often not voluntarily chosen, that it makes fun, is a leisure activity, and I do not go to a certain work place, that data are always created, we have to do nothing special for this (such as working), and finally that it creates no value.

For instance interviewee 9 argues in response to our question whether there should be compensation in exchange for the usage of personal data on SNS:

> *"Actually I think it is consistent per se, when one gives something then one usually gets something in return. I would never guess demanding money for using SNS. Because, for me, this is a private issue and not work; hence job."*

Contrary to the social factory hypothesis, the traditional separation between work time (obviously associated to the public) and leisure time (obviously associated to the private) is crucial for interviewee's argument. An interesting interpretation of the analogy between using SNS and work provides interviewee 17. S/he argues:

> *"I think the comparison is correct because [through using the SNS] you receive needs and you have to work in order to satisfy them. You don't work while using the SNS but you have to work more to feel as comfortable as before because your needs increased. That is in favour not only of Facebook but also of those corporations that do advertising."*

Interviewee 17 links the work analogy to his argumentation that advertising manipulates users and creates unwanted needs.

However following the view of the interviewed SNS users, the abstract concept of "the work of being watched" (Andrejevic 2002) and probably immaterial labour at a whole lacks immediate empirical evidence among the objectively exploited population of SNS users. This is not surprising if we remember the previously introduced qualities of immaterial free labour that include "forms of labor we do not immediately recognize as such: chat, real-life stories, mailing lists, amateur newsletters and so on" (Terranova 2000, 38). Obviously immaterial labour and "the work of being watched" do not fit to dominant experiences interviewees have when they are thinking on work. The problems of immaterial labour also play a crucial role for alienation on SNS; hence we could use the work analogy made in our interview guide also to explore potential aspects of alienation on SNS. Lazzarato argues (1996, 134) that there is an increasing autonomy within the immaterial work process because subjectivity have to be put to work. Subjectivity depends on a series of activities, such as creativity, getting involved with social relations, self-expression, spontaneity, decision mak-

ing activity, learning, cooperation etc. These qualities are commonly associated with freedom, hence non-alienation. Christian Fuchs says in the context of SNS that "labour and play intersect, they create new forms of exploitation" (2011a, 304). Although we found that using SNS is not perceived as work, and this empirical evidence of subjective de-alienation is, as we have seen, mirrored in the theoretical discussion whether there is alienation on SNS, we cannot simply deduce that immaterial labour theories and those theories that see ongoing alienation on SNS are wrong. Subjective perceptions of non-working and de-alienation can come along with objectively being exploited. Furthermore, these subjective perceptions help to intensify objective exploitation because the potentiality of resistance by the exploited is weakened.

As we have discussed the question of exploitation and potential compensation for the usage of personal data on SNS, we touched upon the question whether privacy can be exchanged. In fact, there is a commodification of privacy by the commercial SNS provider, which sells it in exchange for money to the advertising industry. Therefore users' demand of compensation payments can be interpreted as evidence that they feel exploited. Additionally to this, commodification has a further aspect, which rests not with the structural level of SNS providers, but with the individual users. It is described by Campbell and Carlson (2002, 588; see also Comor 2011) as the ongoing "reconceptualization of privacy in the consumer's mind from a right or civil liberty to a commodity that can be exchanged for perceived benefits" and refers to privacy-user benefits trade-offs too. Only if privacy is deemed exchangeable, trade-offs work like interviewees have reported in our study. Would it be rendered as un-exchangeable in society, privacy-trade-offs would have other preconditions. To except privacy from being traded means that it cannot become a commodity and the surveillance based capital accumulation of commercial SNS would not work. Among those who does not want compensation the argument that privacy should not be for sale was influential. We tried to explore this alternative emancipatory approach by confronting interviewees additionally with IQ30 and ask them whether they would sell their personal data in exchange for money or premium options on the SNS.

case	Attitudes towards selling personal data in exchange for money or "premium options"	Attitudes towards compensation payments to the users
1	Can be sold	Wants compensation
2	Should not be for sale	Does not want compensation
3	Should not be for sale	Does not want compensation
4	Can be sold	Does not want compensation
5	Should not be for sale	Does not want compensation
6	Ambiguous	Does not want compensation
7	Should not be for sale	Wants compensation
8	Can be sold	Does not want compensation
9	Should not be for sale	ambiguous
10	Can be sold	Does not want compensation
11	Should not be for sale	ambiguous
12	Can be sold	Wants compensation
13	Should not be for sale	ambiguous
14	Should not be for sale	Wants compensation
15	Should not be for sale	Wants compensation
16	Should not be for sale	Does not want compensation

17	Should not be for sale	Ambiguous
18	Can be sold	Wants compensation
19	Can be sold	Ambiguous
20	Should not be for sale	Does not want compensation
21	Should not be for sale	Does not want compensation
22	Can be sold	Does not want compensation
23	Should not be for sale	Does not want compensation
24	Should not be for sale	Wants compensation
25	Should not be for sale	Does not want compensation
26	Can be sold	Does not want compensation
27	Should not be for sale	Does not want compensation
28	Can be sold	Ambiguous
29	Should not be for sale	Does not want compensation
30	Can be sold	Wants compensation

Table 13: Attitudes towards the sale of personal data and compensation in exchange for the usage of personal data

18 out of 30 interviewees argue that privacy should not be for sale, 11 interviewees say that it can be sold, and 1 interviewee is ambiguous towards this question. Those who argue against selling personal data in exchange for money or premium options on the SNS mostly refer to a principle decision: Something like privacy should not be traded at all; this would be like selling my own person. They also argue that once it is allowed to sell personal data, a bad dynamic arise and privacy would be abolished ultimately. Few interviewees argue in that context that they do not rely on the money and would therefore not engage in selling personal data. Additionally, if selling privacy would be allowed it would affect in particular the poorer; they may be dependent on the money and it would be taken advantage of their situation. Those who argue in favour of selling personal data, first, pragmatically state that SNS provider do it anyway hence it is better to take money for it. Second, they argue that advertising shows no negative consequences for them (see above). Third and most influential they argue that it would depend on the quality and quantity of data in question, on the one hand, and on the amount of money they will receive for their data, on the other hand. Therefore they argue in favour of selling privacy under certain circumstances, but do not suspend the opportunity.

It is salient that in response to IQ30 more interviewees (18 out of 30) argue that privacy should not be for sale than they do in regard of the compensation issue (IQ32). We speculate that this is due to the more active behaviour asked about in IQ30. Here the user actively engages in a privacy exchange whereas in IQ32 the user passively finds the fact that SNS providers do already privacy exchanges. The observation that interviewees insist on privacy as non-alienable, non-exchangeable persona right (Shepherd 2012) may have to do with their cultural background. Differently from the U.S. context, in Europe privacy is traditionally seen as a non-alienable aspect of personality (van Dijk 2010).

We related both categories, “attitudes towards selling personal data in exchange for money or ‘premium options’” and “attitudes towards compensation payments to the users” and found that there are a notable number of 10 interviewees who disagree with both proposals.

	Privacy can be sold	Privacy should not be sold	ambiguous
Wants compensation	4	5	
Does not want compensation	5	10	1
ambiguous	2	3	

Table 14: Relation between willingness to sell personal data in exchange for money or 'premium options' and attitudes towards compensation payments to the users

Interviewee 17 argues in this context and in response to the question about compensations payments:

"Actually that is the same as you asked before; namely whether one agrees with receiving something in return when s/he receives targeted advertising. Of course it would better to be paid than not to be paid. But, I think, the best is not to disclose these information [...]."

We interpret a principle that "privacy should be not for sale" is of overall importance for those 10 interviewees (although only 4 interviewees mentioned it in the context of the compensation question). This principle leads to negative attitudes towards both issues.

Nevertheless, we hypothesised, following the often remarked resemblance between privacy and private property that users see privacy as private property and we are able to find support for this hypothesis too, due to the following reasons:

- We found a dominance of individual privacy notions that neglect societal/transsubjective privacy definitions. Just as private property, so privacy becomes within these notions the right to exclude others.
- We found that users' privacy notions are frequently based on the control theory, which is characterised by subjective formalism. The indifference towards the content of privacy facilitates the individual alienation of privacy.
- We found evidence that property related information, such as financial or business information are deemed private by users.
- We also found concrete willingness to sell privacy among our interviewees, just like private property can be alienated.
- We found in this context that some users are willing to receive an income for the usage of their private data (users want compensation for the usage of their data), just like it is recognised when it comes to the alienation of private property.
- We found that some users see privacy basically as inalienable persona right. However this position may refer back to the possessive individualistic notion of man. Macpherson argues that the selling of individual capabilities, such as one's labour force and we can add one's personal data, presumes an aspect of personality that is inalienable so that regress in slavery is blocked (1962). Carol Pateman argues that this division between alienable individual capabilities and inalienable self is a "political fiction" (2002, 26). She further argues that in fact if labour force or personal data is alienated then also the self is alienated, and if it

happens it is a form of "civil subordination" (2002, 33). We speculate that treating privacy as inalienable persona right is not sufficient to avoid exploitation ultimately. Note that a number of interviewees state that personal data should not be traded in principle, but do not have a sense of exploitation on SNS.

4.5. Privacy trade-off strategies and user alienation

Ellison et al. (2012) have conducted a qualitative study about trade-off strategies that SNS users employ in order to balance the tension between privacy needs, on the one hand, and benefits that are generated through the SNS usage, on the other hand. They describe three strategies for managing audiences: Adjusting their friending behaviours, that is to consciously reflect on which relationships are accepted on SNS; making privacy settings, that is regulation who can see what information about me; and limiting the information disclosure that is the lowest common determinator strategy for users: only information is disclosed that is seen as appropriate for all potential audiences on the SNS. Contrary to the study at hand, Ellison et al. (2012) do not take into account institutional, economic surveillance – which is a general lack of the empirical surveillance and privacy literature. Therefore, their observed strategies cannot simply be adopted four our purposes. The strategy of adjusting friending behaviour does not affect the economic surveillance threat that comes from the SNS provider. As users cannot regulate surveillance for advertising purposes effectively by making privacy settings and the SNS provider is in any case able to collect and process user data regardless which privacy setting users have made (SNS provider own the means of surveillance), this strategy is also of limited relevance in context of our study. The only thing SNS users can do is to limit their information disclosure, no matter if they are SNS literate or not.

We asked users how they balance the privacy issue against user benefits (IQ 21) and indeed the strategy of limited disclosure is the most influential among our interviewees (19 interviewees applied it) and helps them reaching a point where they say that the benefits of SNS outweigh the surveillance and privacy threats clearly. 8 interviewees clearly state that for them the benefits outweigh the threats without pointing to the limited disclosure strategy; interviewee 8 is an example, s/he argues:

"It is a kind of normal thing for us, we are not confident about it, but agree anyway. One is balancing: OK, they are selling my data or I can chat with my friends in the US regularly. And then one says: OK, I prefer to chat with my friends."

Not surprisingly among those (2 interviewees) who have quit using SNS, a negative trade-off result is dominant. These cases highly value privacy and think that it is too exhausting to steadily consider which information is OK to post, and to decide which information should reach which audiences. A further, but rarely employed, trade-off strategy that we have found in our interviews can be termed "subversive usage". Interviewees who employ this strategy are making false statements, using pseudonyms or separate email addresses, and propagating critical, "subversive" information about the SNS on the SNS. Subversive information is for instance information about effective

privacy protection opportunities, about SNS caused censorship, or about alternative SNS. Interviewee 16 argues in the context of a privacy-user benefit trade-off:

> *"Here is a contradiction, no question. The most of what you do is contradictory. It is a trade-off. [...] Facebook would harm me more if I was not on Facebook. I mean that you can share Facebook critical information on Facebook without any problems [...]. Then I can reach a substantial bigger audience than I would publish the information on my blog."*

Some of our interviewees are using browser applications that block advertisements and make them invisible to them. We interpret the usage of ad-blocker software as closely connected to the subversive trade-off strategy.

case	Trade-off strategies
1	Threats outweigh benefits
2	Heteronomy; benefits outweigh threats
3	privacy settings; dynamic nature of trade-off; heteronomy
4	limited disclosure; dynamic nature of trade-off
5	Benefits outweigh threats; limited disclosure
6	Heteronomy; benefits outweigh threats
7	Subversive usage; Heteronomy; limited disclosure
8	Heteronomy; benefits outweigh threats
9	Threats outweigh benefits; limited disclosure; dynamic nature of trade-off
10	Heteronomy; benefits outweigh threats
11	Limited disclosure; benefits outweigh threats
12	Limited disclosure; benefits outweigh threats; Heteronomy
13	benefits outweigh threats
14	Limited disclosure; Heteronomy
15	Limited disclosure; benefits outweigh threats
16	Limited disclosure; benefits outweigh threats; Heteronomy, dynamic; subversive usage
17	benefits outweigh threats
18	Privacy settings
19	Limited disclosure; benefits outweigh threats
20	Limited disclosure; dynamic nature of trade-off
21	Limited disclosure; dynamic nature of trade-off
22	Limited disclosure
23	Limited disclosure
24	Limited disclosure; Heteronomy
25	Privacy settings, benefits outweigh threats; dynamic nature of trade-off
26	Limited disclosure
27	Heteronomy; privacy settings; limited disclosure; dynamic nature of trade-off
28	Heteronomy; privacy settings; limited disclosure
29	Benefits outweigh threats; limited disclosure; dynamic nature of trade-off
30	Privacy settings; benefits outweigh the threats

Table 15: Trade-off strategies and their circumstances

It was said that SNS users do not own and control the means of surveillance, the technological infrastructure where on SNS are based. Therefore some of users' trade-off strategies that other studies have found do not apply to targeted advertising on SNS. Users have to deal with the fact that commercial SNS sell their privacy. According to our critical theoretical approach, we are also interested in aspects of alienation on SNS. Can aspects of alienation be found on SNS? We found some evidence of it in the (limited range of) trade-off strategies that users usually employ when they partic-

ipate in SNS. Interestingly in respect of alienation on SNS, interviewees shared several reflexions about the conditions of their trade-off strategies with us. Besides, pointing to the dynamic nature of their trade-offs (that their trade-offs will change when their life situation changes, that the positive outcome of the trade-off is quite fragile, and that negative publicity will alter the trade-off), a good third of our sample argues that there is a kind of heteronomy that determines the outcome of their assessments. What interviewees mean with heteronomy?

First, they state that they have a lack of knowledge about how their data is processed exactly and that there was no informed consent to the SNS' terms of use and privacy policy. Second, interviewees see a sort of dependency on SNS. They say that it is impossible to waive all the social contacts and relations because it would denote a social exclusion for them. Interviewee 10 uses SNS for business too; s/he works in the culture industry and argues:

> *"That makes me angry [the deficient privacy protection by the SNS provider]. Actually, unsubscribing would be a poor option for me. It is not vital, but it is hardly possible for me. In certain fields I would no longer able to interfere. But actually it is necessary for me and I also want it. There a constant changes and I have to invest time to deal with them, then I think that it is totally futile. It is evermore broadened and one has to protect oneself all the time, well, I find it very exhausting too." Interviewee 14 argues in that context: "Well, it is peer pressure to be in. Well, today there are only a few people who are not on Facebook and remain resistant. One wants to be part of the community hence we have to accept it."*

Third, interviewees feel powerless because there is only in or out and no real opportunity to make differentiated decision, such as an opt-out opportunity for advertising (see below). The SNS also burdens all the responsibility to protect privacy on the user, in their view. Fourth, they argue that there is a lack of alternatives to Facebook's monopoly, which points us to alternative SNS (see also below). Interviewee says in this context:

> *"Simply, the point is that there is no alternative."*

Fifth and finally, we observed a kind of fatalism among the interviewees that can be interpreted as an experience of heteronomy too. In this context interviewees argue, for instance, that nothing is for free in life, that the situation will always be like it currently is, and that they as members of the Internet generation are simply used to give up privacy and to accept surveillance. Interviewee 12 argues for instance:

> *"I think I am not able to change the situation, I will not be able to prevent it [the usage of personal data]." Interviewee 28 assists: "It is always difficult, if you want to use a service, you have to lower your sights. Well, you never will find a SNS that is ideal." Interviewee 8 shows a kind of fatalism in his/her answer: "Meanwhile, it has reached a point, where all are thinking that there are so many data about us around, it doesn't matter anymore. I believe this has to do with the situation that we don't realise what is going on. I don't realise which data they took from me, I*

don't realise to whom they are sold, I don't realise how they are processed, I don't realise how many put their hands on them. And then there is the feeling that you are one out of a million."

To further clarify the circumstances within which SNS users have to do trade-offs and their potential heteronomy, we asked interviewees about their attitudes towards privacy protection through SNS provider (IQ19, 20, and 21). This also includes their opinion of the SNS's terms of use and privacy policies (see section 4.5). Interviewees who think that their privacy is well protected by the SNS provider applied the following arguments: First, they argue that they have made no negative experiences and therefore conclude that the SNS provider protects their privacy well. Second, they argue that SNS providers are exogenously controlled, for instance changes in the terms of use and privacy policies are adaption to the law or taking place due to public pressure. Interviewee 6 argues in this context:

"Of course I know that Facebook could do something bad but I think that they will not do it as it is not their interest. […]Facebook it is used by so many people, I trust that, if there are any major concerns, then some people, for instance the media, would realise it"

Third, users argue that SNS providers take their privacy needs seriously because SNS have implemented differentiated privacy setting opportunities, steadily take care of improving the site, voluntarily subject themselves to data protection rules, and try to meet user complaints. Therefore the negative publicity about SNS is mainly fear mongering. For instance interviewee 5 argues this way when s/he was asked why changes in the terms of use and privacy policies are taking place:

"Well, if this are change in order to improve the thing, or to protect the data from the outside, then I think it is positively." Likewise interviewee 19: "Ok if I have read it correctly then the last changes were improvements, I think. Perhaps, it goes too little in this direction, but anyhow in the right direction. You have mentioned Facebook's branch in Europe: Now a stronger pressure exists to stick with the valid legal situation. In principal I think this legal situation is a good one, Europe surely has a more essential approach to data protection and privacy than it is the case in the USA. Hence it is not the worst." Interviewee 25 says in this context: "Initially I think I should look up the changes, when somebody is posting about it. But then a different information comes in mostly that says all before was fear mongering and nothing is really changing. Then I feel reassured."

case	Attitudes towards privacy protection through SNS provider (applied arguments)
1	Ambiguous (No privacy on the Internet; SNS takes privacy seriously)
2	Negative (No privacy on the Internet; dishonesty)
3	Negative (Dishonesty; Profit orientation inhibits privacy protection; in-transparency)
4	Negative (In-transparency; SNS is not controlled)
5	Positive (SNS takes privacy seriously)
6	Positive (SNS is exogenously controlled)

7	Negative (In-transparency; No privacy on the Internet; dishonesty)
8	Negative (SNS is not controlled; Profit orientation inhibits privacy protection)
9	Ambiguous (No privacy on the Internet; Profit orientation inhibits privacy protection; SNS takes privacy seriously)
10	Negative (No privacy on the Internet; in-transparency)
11	Negative (Profit orientation inhibits privacy protection; in-transparency; dishonesty)
12	Positive (No bad experiences; SNS takes privacy seriously)
13	Positive (SNS is exogenously controlled)
14	Ambiguous (In-transparency; SNS takes privacy seriously)
15	Positive (SNS is exogenously controlled; no bad experiences; SNS takes privacy seriously)
16	Negative (Profit orientation inhibits privacy protection; SNS is not controlled; dishonesty)
17	Negative (No privacy on the Internet; Profit orientation inhibits privacy protection; dishonesty; in-transparency)
18	Ambiguous (SNS takes privacy seriously; SNS is not controlled; in-transparency)
19	Positive (SNS takes privacy seriously; SNS is exogenously controlled)
20	Positive (No bad experiences)
21	Ambiguous (In-transparency; dishonesty; no bad experiences)
22	Positive (SNS takes privacy seriously)
23	Ambiguous (In-transparency; dishonesty; SNS is not controlled; SNS takes privacy seriously)
24	Ambiguous (In-transparency; dishonesty; SNS is exogenously controlled)
25	Positive (SNS takes privacy seriously)
26	Negative (In-transparency; dishonesty)
27	Ambiguous (In-transparency; dishonesty; Profit orientation inhibits privacy protection)
28	Ambiguous (Dishonesty; SNS takes privacy seriously; SNS takes privacy seriously)
29	Ambiguous (No privacy on the Internet; no bad experiences; Profit orientation inhibits privacy protection; dishonesty)
30	Ambiguous (SNS takes privacy seriously; Profit orientation inhibits privacy protection)

Table 16: Distribution of arguments regarding attitudes towards privacy protection through SNS provider

On the contrary, interviewees who think that their privacy is not well protected by the SNS provider apply the following arguments: First, they argue that privacy cannot be ensured in the Internet in principal, therefore SNS providers' privacy protection must be deficient. Second, they contend that the SNS are not controlled either by the participation of users or external institutions. Interviewee 16 argues that

> *"if it would be a SNS that is run by the university […], then I would put more confidence in it, it would be not so unfamiliar then." Interviewee 7 argues accordingly: "Facebook always set the situation and then voices are raised that oppose and argue that Facebook has to change the situation so that it is legitimate. Facebook steps forward and then backwards, they apologise but do it anyway." Interviewee 16 argues likewise: "Interviewer: Have you read Facebook's terms of use and privacy policy?/ Never and I think I will not read it in the future too./ Interviewer: Why that?/ It is paper that doesn't blush, I would not understand two third o fit because it consists of legal expressions. If I would realise that Facebook behaves inappropriate then this would be of no use for me. They simply do it. I would have to be proactive. Either I upset and will be ignored, then I upset again and will be ignored again, then one can try to pressure the corporation on the site so that Facebook fears consequences or one hast o go to law. I, surely, will not go to lay because I have to less money and time for it. In comparison what they claim, the company does inappropriate things by all means, but no one notices it. Well I have little trust in it, and that is something what is confirmed by the media all the time. […] All things considered, I assume that I'm not satisfied. You can put it in a populist way: I have a general suspicion."*

Interviewee 7 and 16 not only points to the lack of effective control over SNS providers, s/he also mentions their dishonesty. We are able to identify a third line of argumentation: SNS behave dishonestly and non-truthful, in fact they do not want to protect user's privacy. Interviewee 27 argues in this context:

"It may be that they intended to disclose more from the very beginning. In the beginning they didn't want to reveal it, they wanted to pretend to be a good system. But then they secretly made all visible [...]. Perhaps due to economic purposes, perhaps for advertising; perhaps they have contracts with Internet companies, which are keen to access it."

The fourth argument that is applied by users to criticise SNS provider's privacy protections points to intransparency. The SNS do not make clear what they do with the user data or how users can protect their privacy. The terms of use and privacy policy is not understandable and the SNS do not inform the users about changes of these documents appropriately. A fifth strand of argumentation says that SNS' profit orientation inhibits effective privacy protection. Interviewee 11 says in that context:

"Of course it is visible as much as possible in order to be attractive for advertising customers. Also the privacy settings are extremely inconvenient and all is very difficult and not much transparent." Interviewee 17 argues: "Well, most of the time you simply do not realise when somebody is accessing your site. You do not know how much you are surveiled. In particular the founder [of Facebook] pretended to be a philanthropist and that he would not sell to big corporations. One day he sold half of a per cent and then it becomes more and more. He has always pretended that he is not interested in money; therefore he had the advantage towards competitors. [...] and he had the people's trust, at least in Germany and partially. Surely the confidence was betrayed because it came to public what is really happening with the data."

It is salient from our material that interviewees have more points of critique towards the terms of use and privacy policy than they have according the overall privacy protection through the SNS provider. The influential arguments about the intransparency of how and if privacy can be protected refers to deficient privacy policies and the terms of use.

To sum up the previous theoretical discussions about alienation on SNS and our empirical results, we can asses that there are at least three different concrete forms of alienation on SNS:

- First, there are clearly limitations in SNS user's decisional freedom. This becomes obvious when interviewees state that they have a lack of knowledge and have not given an informed consent to the SNS terms of use. Several authors (e.g. Fernback and Papacharissi 2007; Sandoval 2011) have outlined that SNS do not foster informed user content; rather intentionally impede it. This situation gives some evidence of the first concrete appearance of alienation on SNS.

- Second, indeed SNS users may be free to chose, but they are not free to determine the spectrum of potential decisions. Empirical evidence for this form of alienation is given when users point to a loss of the "social" in social networking, for instance, when advertisements pop-up on the users' wall where they usually receives information about friends. Another obvious aspect in this context is that users only have "sink or swim" opportunities regarding acceptance of terms of use and potential changes, as well as regarding their acceptance of advertising and economic surveillance. The limited disclosure strategy is also notable here because it means that users have to relinquish some social benefits that are inherent to SNS.
- Third, there are indirect forms of limiting users' freedom on SNS that are harder to access empirically. In the theoretical discussion it is referred to them as self-governance, self-disciplining, and self-surveillance in the context of immaterial labour on SNS. We speculate that users' fatalism and the very acceptance of the status quo could be expressions of alienated self-governance. We interpret that the borrowing of SNS provider interests by SNS users is an instance for this form of alienations. Another aspect is that interviewees also welcome targeted, hence surveillance-based advertising on SNS, not only because they do not fear privacy invasion, but also because they think that targeted advertising provides useful information, respects and takes my needs seriously, and allows me to participate in which advertisements are confronted to me. We also can add here the strong line of argumentation about the manipulating effects of advertisements on SNS.

4.6. Alternative SNS

A dialectical analysis of society, that shows the interplay between advantages and disadvantages, is needed for interpretation of empirical research. Such analysis wants to show that the situation of disadvantages' primacy over advantages is societal shaped and therefore possible to change. Which solutions to the problem of exploitation and alienation on SNS may be realistic for effectively realising the mentioned user suggestions? Fuchs (2011d), Allmer (2011), and Sevignani (2012) propose to support alternative, non-commercial SNS. Taking alternative SNS into consideration one can imagine alternatives to the discussed trade-off strategies on SNS. In this section, we explore users' attitudes towards alternative SNS. We do this on behalf of three concrete issues. First we ask for user's suggestions for a good, privacy-aware SNS. Second, we explore what they think about alternative funding models. Third, we introduce to them existing alternative SNS and ask them what they think about these alternatives.

We asked interviewees what they wish an SNS should include in its terms of use and privacy policy (IQ19 and 20). Users make the following suggestions:

- SNS should ensure that there is a informed consent to changes on the SNS;
- they wish a deleting of data after a certain period of time or of old data after changes were made;
- they suggest that the SNS does no statistical analysis of the users' data;

- the SNS should not disclose data to third parties, in particular it should not sell user data;
- personal data should not appear elsewhere than on the genuine site;
- user should remain perfect ownership of uploaded data;
- they wish clear and concise terms of use and privacy policies.
- They further suggest traditional instead of targeted advertisements;
- and that the SNS makes no own suggestions of potential friends to users;
- finally, that the SNS should not perform face recognition of its users.

Additionally, users frequently suggest SNS to ensure that privacy settings also apply to advertising. We explored this suggestion in more detail by asking interviewees, after we have explained them the differences between opt-in, and opt-out mode to organise agreement to advertising, which mode they would prefer (IQ32). For instance Facebook has currently only a few settings options for advertising (in their view, advertising is however not a privacy issue, therefore they do not call it privacy settings). Facebook users must become active in opting-out from some sorts of advertising (e.g. social advertising). As mentioned before, there is no opt-in opportunity for it and especially no opt-in opportunity for advertising in general.

case	Introduction of opt-in opportunity for advertising on SNS	Introduction by law	Further user suggestions
1	Yes (conflict of interest)	Yes	No data disclosure to third parties
2	Yes (conflict of interest)	Yes	Informed consent to changes
3	Yes (user advantages)	Yes	other
4	Yes (conflict of interest)	Yes	Informed consent to changes
5	Yes (conflict of interest)	Yes	Informed consent to changes
6	No	No	Deleting of data; Informed consent to changes; Clear and concise terms of use and privacy policy
7	Yes (user advantages)	Yes	Clear and concise terms of use and privacy policy
8	Yes (user advantages)	No	Informed consent to changes
9	Yes (conflict of interest)	Yes	-
10	Yes (user advantages)	Yes	Clear and concise terms of use and privacy policy
11	Yes (user advantages; adoption of SNS provider's interest)	No	Informed consent to changes; No data disclosure to third parties
12	Yes (user advantages)	Yes	Informed consent to changes; no statistical analysis of user data
13	Yes (user advantages; adoption of SNS provider's interest)	Yes	-
14	Yes (conflict of interest)	Yes	Informed consent to changes
15	Yes (user advantages)	No	No data disclosure to third parties
16	Yes (user advantages)	Yes	Informed consent to changes
17	Yes (conflict of interest)	Yes	other
18	Yes (conflict of interest)	Yes	-
19	Yes (user advantages)	Yes	-
20	Yes (user advantages)	Yes	-
21	Yes (conflict of interest)	Yes	No data disclosure to third parties
22	Yes (user advantages)	Yes	Informed consent to changes
23	Yes (conflict of interest)	Yes	Other; Informed consent to changes
24	Yes (user advantages)	Yes	No data disclosure to third parties; Deleting of data; Informed consent to changes
25	Yes (conflict of interest)	Yes	No data disclosure to third parties; Deleting of data
26	Yes (conflict of interest)	Yes	Clear and concise terms of use and privacy policy
27	Yes (conflict of interest)	Yes	Informed consent to changes
28	Yes (user advantages)	Yes	no statistical analysis of user data; Clear and concise terms of use and privacy policy
29	Yes (user advantages)	Yes	-
30	Yes (conflict of interest)	Yes	-

Table 17: User suggestions for (alternative) SNS

The results are that only one out of 30 interviewees does not want the opportunity to enable first, before data can be used for advertising. Interviewee 6, who does not want to introduce the opt-in mode, argues:

"No, I think it is more important to introduce an obligation to inform the users. […] It is not enough to simply inform the users somehow; instead they should be informed about certain issues very clearly and explicitly. So that people know what they can change and how they can do it. Whether the default settings are enabled or disabled is then not that important in my view. I can then argue that it was the decision made by the people, they knew and if they are too lazy to change something then it is bad for them and good luck for Facebook. But it was not a violation by Facebook."

The overwhelming majority does support the introduction of opt-in and would even welcome a law which makes opt-in for advertising mandatory (26 interviewees). We are able to identify three lines of argumentation according this issue: First, there should be no or at least no mandatory opt-in for advertising usage of personal data. Following the argumentation of interviewee 6, these users also (partly) adapt the SNS provider's interest. This is very obvious in the initial response of interviewee 8 to the question whether the opt-in should be mandatory introduced:

"I don't know it exactly. That is a kind of a difficult question when juridical rules in the economy are at stake./ Interviewer: What do you mean?/ Well, it is an invasion into the free market system."

At least at the quoted beginning of his/her response, interviewee 8 does not care about user interest, but cares about the abstract economic system and the consequences that a law would have for the SNS provider. Interviewee 11 argues similarly in response to the same question:

"That is a difficult question … I tend to say no because I think that it is not possible for the firms to sustain their business."

Interviewees 11 and interviewee 13 have the same concerns, but draw different consequences. Interviewee 13 argues:

"It would be not bad to think about it./ interviewer: why?/ It would be mandatory for everyone. If that would be the case then it would be not that bad for them [SNS providers] because then nobody receives the data and for us it would be better if all that is not in the Internet."

Second, users do not recognize an explicit conflict of interest between them and the SNS providers at this point. They, however, stress the advantages or reliefs that users would have if the opt-in mode is realised. They may or may not argue for a law. In this context it is argued that such an opportunity makes less work for the users and pro-

tects the careless among them. It also could be avoided that data can be used without explicit consent for a short period of time. They also argue that the opt-in would make it explicit that there is surveillance for advertising purposes on SNS.

Third, users clearly see a conflict of interests between them and SNS providers. They argue in favour of a law as they know that SNS would not introduce the opt-in mode voluntarily because this would contradict SNS providers` profit interests. Interviewee 17 expresses this:

> *"This would make sense. People want use Facebook out of practical reasons and they do not want to care about other things. This is exploited due all is activated by default and one have to invest a lot of time to deactivate it. […] Yes absolutely because such a site has a monopoly which is taken advantage from all the time. Hence there should be provisions by law." Interviewee 2 assists: "Absolutely let's introduce the law: Currently it is aimed at the stupidity and laziness in order to gain profit." Likewise interviewee 27: "It would be not bad. But can they survive then? I don't know if somebody will click on them then. That would be quite a disadvantage for them. However, I would plead for it."*

According to our critical theoretical approach, the fact that the users cannot realise the mentioned needs to decide about the conditions within which they use SNS by themselves points to an alienated situation within which they have to act. That they cannot opt-out from advertising is a particular aspect of alienation because it forces them to contribute to their own exploitation.

We found not surprisingly that all those interviewees who disagree with advertising on SNS plead for a mandatory opt-in at the same time. In addition nearly all interviewees who have ambiguous attitudes towards advertising on SNS also want an opt-in opportunity to be introduced mandatory.

	Agreement with advertising on SNS	Disagreement with advertising on SNS	Ambiguous attitude
Mandatory opt-in	10	6	10
No mandatory opt-in	3	0	1

	Advertising on SNS is a privacy invasion (before information input)	Advertising on SNS is not a privacy invasion (before information input)	Ambiguous attitude
Mandatory opt-in	11	12	3
No mandatory opt-in	0	3	1

Table 18: Attitudes towards the introduction of a mandatory opt-in opportunity for targeted advertising on SNS in relation to attitudes towards advertising on SNS and attitudes towards advertising on SNS as a privacy issue

All those interviewees who think that advertising on SNS is a privacy invasion clearly want a mandatory opt-in for advertising on SNS.

Above all the alternative character of an SNS is determined by a funding model that is not based on user surveillance. Hence funding cannot easily ensured by advertising. We asked interviewees of several alternative funding, namely donation funding, tradi-

tional payment funding, and public funding models for SNS (IQ34). A potential public funding model for SNS gains least support (5 interviewees support it; 3 have ambiguous attitudes towards it). Frequent arguments why interviewees challenge a public funding model for SNS are: First, not everyone uses SNS but the costs have to be afforded by all. Second, interviewees argue that there is no public interest in providing SNS, they already exists without public funding. Obviously the specific (for instance, alienated or exploitative) quality of the SNS does not play a role within this arguments. Given the fact that non-commercial alternative SNS are unknown, this applies in particular. Third, users argue that the state would then influence SNS and should therefore not organise the funding of SNS. The state appears as the only entity that is able to do public funding. On the other hand, those interviewees who support a public funding model apply the following lines of argumentation: First, there is a real public interest: SNS are used by so many and public funding would effectively save costs for society because the costs will be less than the total costs generated by advertising. Second, public funding could help to close digital divides and would avoid exclusion, for instance through social sorting. Third, public funding would enable to make mandatory requirements for SNS, such as better terms of use for instance. Fourth, those who are critical about commercial SNS argue that a public funding model would ensure that SNS become non-commercial.

In regard of direct payments, including donations and traditional pay per use, those interviewees that are against argue that, first, the greatest advantage of SNS, namely that they are a free opportunity to communicate would get lost. Second, interviewees think that SNS as such are not worth or not important enough to pay or donate for them. On the other hand, we found one influential argument why users support to pay or donate for SNS. They argue that it is voluntarily to do so.

case	Attitude towards direct payments	Attitude towards donation funding	Attitude towards public funding
1	supportive	supportive	challenging
2	challenging	supportive	supportive
3	Challenging	Supportive	supportive
4	ambiguous	supportive	challenging
5	supportive	supportive	challenging
6	challenging	challenging	challenging
7	challenging	supportive	challenging
8	challenging	supportive	Ambiguous
9	challenging	supportive	challenging
10	ambiguous	ambiguous	challenging
11	supportive	supportive	ambiguous
12	challenging	ambiguous	challenging
13	supportive	challenging	challenging
14	challenging	challenging	challenging
15	challenging	challenging	challenging
16	challenging	supportive	challenging
17	supportive	challenging	supportive
18	Challenging	challenging	challenging
19	supportive	supportive	supportive
20	Challenging	challenging	challenging
21	supportive	supportive	ambiguous
22	challenging	challenging	challenging
23	Challenging	Supportive	challenging
24	supportive	supportive	-

25	supportive	challenging	challenging
26	challenging	challenging	challenging
27	supportive	supportive	supportive
28	supportive	challenging	challenging
29	challenging	-	-
30	challenging	supportive	Challenging
TOTOAL	Supportive: 11 Challenging: 18 Ambiguous: 1	Supportive: 16 Challenging: 11 Ambiguous: 2	Supportive: 5 Challenging: 20 Ambiguous: 3

Table 19: Attitudes towards alternative funding models for SNS

Frequent arguments why interviewees support pay per use models in particular, such as subscription or pay per use, are that it, first, would ensure better data and privacy protection because the personal user data would not be used for advertising. Second they argue that such a funding would mean fewer costs for all. They refer in this context to the method of micropayments and point to less individual costs as an advantage of this method. Third, users argue that there are always costs (also with advertising), but payment per use would make them transparent and understandable to the users. Contrary, those who argue against direct payments, such as subscription or pay per use, apply the following arguments: First, they argue that there will be always a free SNS. Second, they argue that this funding model would results social exclusions. Because then SNS would be only accessible for an elite or for the rich. Third, they fear that the number of users would decrease and destroy the network ultimately.

Frequent arguments why interviewees support donation funding for SNS are the following: First, donation can be made conditional on requirements, such as open source code of the software, no advertising etc. Second, it is voluntary to donate and, third, donations are a social progressive funding model. On the other hand, those who challenge the donation funding for SNS argue that, first, donations are an intransparent funding model and would allow the major donors to influence. Second, the say that donations are not a sustainable funding and the so funded SNS will therefore not survive. Third and related, they point to a free rider effect and argue that willingness to donate will decrease if it is non-mandatory.

Donation funding gains the most support among our interviewees. This is notable because funding through donation is a non-capitalist mode of running a SNS.

As part of our participatory research approach, we provided users with information about existing alternative, non-commercial SNS and asked them what they think about these alternatives (IQ34 – 38). Briefly described examples were on the one hand, Diaspora (see for a detailed and critical discussion Sevignani 2012) and, on the other hand, kaioo. Although Diaspora received some attention and media coverage since in particular Facebook is facing public outcries regarding their privacy irrespective behaviour it was, due to the strong monopoly position of Facebook and Google, hard to find interviewees that were familiar with these kinds of alternatives.

The general knowledge about alternative SNS, which is mirrored in our sample, was absent or nearly absent. In regard to our third research question, we study interviewees primarily as informants and emancipatory actors.

It is salient that all interviewees express a supportive attitude towards the introduced alternative SNS, Diaspora and kaioo. Influential arguments why interviewees support the introduced alternative SNS are the following: First, they think that they embody the real network idea, which surrounds social relationships and community building instead of other purposes, in particular gaining profit. Second, interviewees are supportive because alternative SNS avoid the abuse of personal data and potential state surveillance. Third, because of alternative SNS are non-commercial, free of advertising and therefore do not need centralised power architecture; and fourth these alternatives enable participation, self-organisation, and self-determination (more) effectively. We can observe a close link between the arguments highlighting the non-commercial quality, the participation/self-determination aspect and those which point to the advantage of privacy protection. Fifth, interviewees argue that alternative SNS would establish/ maintain pluralism among SNS providers, which is valued positively per se.

We are further able to differentiate between two forms of user support, one is support in a non-material way and one is monetary support. Whereas all interviewees support alternative SNS at least ideally, the half of our sample (15 out of 30) replied our question whether they would also support alternatives monetarily with a positive statement. The amount of money they would spend varies between less or equal than 10 Euro a year and more than 100 Euro a year; most of the supporters would pay less or equal than 10 Euro a year. This result is very interesting: If only one percent of the one billion Facebook users would switch to an alternative SNS and support it with 5 Euros a year, this alternative SNS would be equipped with 50 million Euros a year. A typical argument against monetary support for alternative SNS is made by interviewee 15

> *"I think that sounds well in principle, personally however, as I find it not that bad that SNS are financed through advertising and we can take advantage form the fact that corporations are financing the SNS for us, I think that donation could be made for more meaningful projects".*

The critical stance towards monetary support puts into perspective but does not withdraw the fact that all of our interviewees show an overall supportive attitude towards alternative SNS.

We were able to observe changes in attitudes towards donation funding during the interview. Earlier we ask interviewees what they think about alternative funding models for SNS, one of them was funding through donations. After we gave interviewees information about two existing alternative SNS which are funded by donations, we ask them whether they would support those alternatives monetary. Six interviewees, who had a challenging or ambiguous attitude towards donation funding before, stated that they now would support the introduced alternative SNS monetary.

But one the other hand also six interviewees who had previously supportive or ambiguous attitudes towards donation funding, state that they would not support alternative SNS monetary. Obviously concrete instances of alternative SNS can alter users' willingness to welcome a donation funding model for SNS. On the one hand, alternative SNS, once they are known, can convince users that monetary support in the form of donations is meaningful. On the other hand, those who support donation funding of SNS on a abstract and general level, are not necessarily willing to spent actual money for alternative SNS – or they are not convinced by the alternative offerings.

Although all interviewees support the introduced concepts of alternative SNS, most of them however express doubts or criticism (in particular those who support alternative SNS theoretically but would not support them monetarily) or at least talk about potential challenges for them (in particular those who would support them also monetarily). Relevant challenges that alternative SNS, in the view of the interviewees, are facing are the following: First, the most frequent challenge that interviewees see for alternative SNS is that the number of their users will be (remain) limited. People are not aware of the existing alternatives and only particularly 'skilled' users, such as informatics or 'IT-nerds', will contribute to the alternatives actively. On the other hand there is a monopoly of Facebook that is based on network effects, that is as many users a SNS has as much attractive it is for potential further users. Second, an influential line of argumentation is to question that the alternative SNS's funding is sustainable. Users think that donations are an insecure funding model. In a way this argument is connected to the third line of argumentation: Interviewees do not trust the non-commercial quality of the alternative SNS. They cannot imagine that nobody will capitalise on the alternatives. They fear a 'creeping' or gradual commercialisation once the SNS are grown. Interviewee 3 expresses this:

> *"It's all about financing, in the beginning, I mean, also Facebook was relatively harmless, and then it surely has gone worse as it has become so big".*

Fourth, interviewees think that new or different power structures will emerge on the alternatives. For instance, major donors or specialists will influence them. Fifth, interviewees fear that participation, self-organisation, and self-determination will turn out to be only formal or superficial. In particular for Diaspora, interviewees see the challenges that real decentrality cannot be realised due to technical limitations or they are unclear whether everybody will be able to run a personal server, which is a precondition of a real decentrality and distributed power structure on Diaspora. On the other hand, they mention that a real decentralised architecture may be disadvantageous because it provides less control to avoid problematic or "dangerous" content, insecurity, and irresponsibility. In particular for kaioo, interviewees raise the question whether there will be any consensus about the terms of use among the users. Table 20 gives an overview about the supportive arguments, kinds of challenges interviewee see for alternative SNS. The table also lists the arguments interviewee have employed to express their (non-)willingness to support alternative monetarily.

case	supportive arguments for alternative SNS	kind of challenges for alternative SNS	willingness to monetary support	Changes in attitudes towards donation funding	arguments against monetary support	prior knowledge about alternative SNS
1	participation/self-determination; non-commercial	real decentrality?; disadvantages of decentrality	≤ 10	no	-	none
2	non-commercial; real social network; participation/self-determination	-	no	Was supportive	-	none
3	participation/self-determination; non-commercial	non-commercial?; number of users	≤ 50	Was challenging	-	low
4	pluralism	non-commercial?	no	Was supportive	not important enough to support; advantages do not weigh enough	none
5	-	no consensus about the terms of use	≤ 50	No	-	none
6	-	number of users; real decentrality?; disadvantages of decentrality; sustainable funding?	no	No	not important enough to support	none
7	pluralism; real social network; participation/self-determination	disadvantages of decentrality, number of users	≤ 10	No	-	high
8	non-commercial	sustainable funding?	≤ 10	No	-	none
9	non-commercial; privacy, real social network	-	no	Was supportive	does not use sns	none
10	real social network	number of users; real non-commercial?	≤ 10	Was ambiguous	-	none
11	non-commercial; participation/self-determination; no abuse of personal data	new power structures?	≤ 10	No	-	high
12	non-commercial; participation/self-determination; no duty to pay; privacy	new power structures?	≤ 50	Was ambiguous	-	none
13	participation/self-determination	sustainable funding?	≤ 10	Was challenging	-	none
14	privacy	new power structures?; disadvantages of decentrality; real participation/self-determination?	≤ 10	Was challenging	-	none
15	participation/self-determination	-	No	No	not important enough to support	none
16	participation/self-determination; privacy	new power structures?; number of users; real participation/self-determination?; sustainable funding?	≤ 10	no	-	high
17	no abuse of personal data; privacy	number of users	≤ 50	Was challenging	-	none
18	non-commercial;	-	no	No	-	none
19	no abuse of personal data; non-commercial	number of users; real decentrality?	no	Was supportive	-	low
20	pluralism	real decentrality?; disadvantages of decentrality; non-commercial?	no	No	advantages do not weigh enough	none
21	privacy; participation/self-determination	-	≤ 10	No	-	none
22	non-commercial; pluralism	real decentrality?	no	No	-	none
23	non-commercial; participation/self-determination	non-commercial?	no	Was supportive	does not use sns	none
24	participation/self-determination; privacy	number of users; disadvantages of decentrality	> 50	No	-	low
25	participation/self-determination; privacy	number of users; sustainable funding?	no	No	-	none
26	participation/self-determination; privacy	number of users	no	No	not important enough to support	none
27	-	sustainable funding?	> 50	no	-	none
28	participation/self-determination	sustainable funding?	no	No	-	none
29	pluralism	number of users	no	No	not important enough to support	low
30	non-commercial; privacy	number of users	no	Was supportive	not important enough to support	low

Table 20: Distribution of supportive arguments, kinds of challenges interviewee see for alternative, and the arguments they employed to express their (non-)willingness to support alternative monetarily (in euro/year)

Those interviewees who solely employ the pluralism argument in order to show their support for alternative SNS at the same time say that they would not support alternative SNS monetary. We interpret the pluralism argument therefore as a weak form of supporting alternative SNS because it does not aim at replacement of problematic SNS with alternatives but aims at supplementing commercial SNS. Interviewee 20, after s/he has spent some time for thinking about challenges for the introduced alternative SNS, says:

> *"Yes absolutely, am I contradictory? I think there should always be an alternative. There should be no monopoly, such as Facebook because then it can be abused". Interviewee 4 assists: "It [having alternative SNS] is not a bad think in principle because it is an alternative. The bigger Diaspora becomes, the much pressure Facebook faces because users will realise that there are alternative that protect their privacy better. In consequence the monopoly position of Facebook is weakened and they know then that they cannot presume to do everything."*

Those interviewees are good examples for a weak support of alternative SNS; with them supporters' thinking about challenges tends to take on the form of substantial doubts and criticism of the introduced models. Additionally all of them agree with advertising on SNS.

Knoche (2003), Sandoval (2009), and Sandoval and Fuchs (2010) have analysed the situation of alternative media today and mention several contradictions that these media usually face within a capitalist society. For instance, Knoche (2003) speaks of a lack of funds, interested audiences, and people who help to produce alternative media. Additionally those who sustain alternative media are frequently confronted with precarious and self-exploitative labour situations. This results in a permanent pressure for commercialisation and for the potential loss of being an alternative.

Most of the challenges that were named by our interviewees (the number of users will remain limited, alternative funding strategies, such as donation will not sustain the alternative SNS, creeping commercialisation, participation, self-organisation, and self-determination will turn out to be only formal or superficial) can be interpreted pointing to objective contradictions alternative media are facing in a capitalist environment. To mention challenges does not meant to be against alternative SNS; rather it means that users recognise (consciously or unconsciously) structural problems of alternative media.

	Agreement with advertising on SNS	Disagreement with advertising on SNS	Ambiguous attitude
Monetary support of alternative SNS	5	6	4
No monetary support of alternative SNS	8	4	3

	Advertising on SNS is a privacy invasion (before information input)	Advertising on SNS is not a privacy invasion (before information input)	Ambiguous attitude
Monetary support of alternative SNS	8	5	2
No monetary support of alternative SNS	3	10	2

Table 21: Attitudes towards the introduction of a mandatory opt-in opportunity for targeted advertising on SNS in relation to attitudes towards advertising on SNS and attitudes towards advertising on SNS as a privacy issue (before the information input)

In general we can say that there is a tendency that those interviewees who disagree with advertising on SNS support the alternative SNS monetary; so do those who see advertising as privacy invasion from the beginning. A contrary tendency can be observed among those who agree with advertising on SNS and do it not perceive as a privacy invasion from the beginning.

4.7. Mentioned consequences of the interview

There was no specific question to explore which consequences the interviewees draw from the interview. Some (9) interviewees however mentioned some consequences for them by themselves. As part of our participatory research approach that aims at societal change, we document them here: On a cognitive level, interviewees mentioned that the interview triggered a reflection process about the current usage of (commercial) SNS and about potential alternative to it. They stated that they have learned something during the interview and will use the issues that were discussed in further discussion with others. On a practical level, interviewees said that they will check their privacy and advertising settings and disable as much as possible. They also stated that they will support alternative SNS in future times.

4.8. Types of SNS users

We supposed that within a critical theory approach SNS users should be studied as informants, socially sorted, excluded, exploited, and other-directed people, as well as caught in an ideological discourse, and emancipatory actors. In the previous sections we have described what our interviewees think about several issues surrounding privacy, surveillance, and advertising on SNS. We also have interpretatively argued that they are exploited, other-directed, and alienated. In the following, we theoretically construct, based on the interview issues, prototypes of the critical SNS user as an emancipatory actor. This type is contrasted by the uncritical SNS users as instances of an ideological discourse.

Foucault (1977) stresses hat surveillance is a technology that exercises disciplinary power in order to sustain domination. Gandy speaks about the panoptic sort as “a difference machine that sorts individuals into categories and classes on the basis of routine measurements. It is a discriminatory technology that allocates options and opportunities on the basis of those measures and the administrative models that they inform” (1993, 15). These different approaches towards surveillance have in common that they see surveillance as a negative phenomenon that is related to domination and power asymmetries. Christian Fuchs provides several reasons why positive and neutral surveillance conceptions fail to be critical of current capitalist societies within which surveillance is mainly performed by powerful actors in order to realise their interests on the costs of the many who are under surveillance and suggest “that the

term surveillance should be employed for describing the negative side of information gathering, processing, and use that is inextricably bound up with coercion, domination, and (direct or indirect; physical, symbolic, structural, or ideological) violence" (2011, 126). According to critical theory of surveillance, SNS users having a negative notion of surveillance and having a sense of hierarchy in the context of surveillance can be named critical SNS users and potential emancipatory actors. On the other hand, SNS users that have neutral or positive notions of surveillance and do not relate surveillance to power asymmetries belong to the uncritical prototype of a SNS user who has ideological views.

The critical SNS user disagrees with advertising in general and on SNS; s/he may argue that targeted advertising is a problematic form of surveillance, pressing, manipulating, and creates (unwanted) new needs, or that it is superfluous and does not add anything meaningful to his/her life. S/he may argue that advertising is opposed to and harms the genuine idea and sense of social networking. On the contrary, the uncritical SNS user agrees with advertising in general and on SNS.

We have argued that the reference to privacy in order to oppose to surveillance and advertising on SNS can be both, critical and uncritical. It depends which notion of privacy is employed. SNS users who see social aspects of privacy and vote for the mandatory opt-in opportunity to advertising on SNS are critical. Uncritical SNS users on the contrary have a possessive, pure subjective, formalistic, and individualistic understanding of privacy. The critical SNS user argues that privacy should not be sold and that it is an inalienable human right. However when s/he recognises that privacy is de facto traded then s/he wants compensation in return for this trading in order to limit commercial SNS provider's power. The uncritical on the contrary has no problem with selling privacy and does not want compensation in return for this selling or thinks that using the site for free is enough of compensation.

The critical type has a feeling of heteronomy when s/he uses SNS; s/he feels other directed and alienated through the SNS provider. On the contrary the uncritical feels completely free when s/he uses SNS and thinks that the SNS provider always acts in the users' interests.

The critical SNS user supports alternative SNS that are non commercial and break with power asymmetries between the user and the provider. The critical SNS user is willing to support alternative not only ideally, for instance he would – according his/her capacities - donate money to the alternatives. The uncritical does not support alternative SNS or support them only ideally, for instance as he is interested in a general pluralism of SNS providers.

5. Conclusion

In this section we summarise the main results of our study according our research questions and hypotheses.

RQ1.1: Which arguments do students use for arguing that they disagree/agree with certain kinds of surveillance on SNS? In the opinion of students who are critical of

surveillance on SNS, who or what aspects of life and activities should be protected from surveillance on SNS?

We found that interviewees most often link surveillance to corporations (22 out of 30 interviewee), the state (20 out of 30 interviewees), and in general various technologies that allow certain entities to surveil, such as the Internet or surveillance cameras (14 interviewees).

We found that pure positive notions of surveillance are empirically little anchored and those who stress the negative character of surveillance, argue that it is a privacy invasion, secures existing power inequalities through control, exploitation, and manipulation. These results support the relevance of a critical theory of surveillance (Allmer 2012; Fuchs 2011f, 2012).

Hypothesis 1a: A typical attitude expressed by SNS users is that they are unconcerned about the use of their data for economic ends because this form of surveillance is mainly invisible and does not show direct visible effects.

Economic aspects are most frequently linked to the term surveillance.

Interviewees associate employer surveillance just as often as they associate advertising with the term surveillance. 13 interviewees are critical of employer surveillance (does worry and/or do not like it) and 10 interviewees disagree with targeted advertising before we gave our information input. Hence we were not able to detect significant differences in users' overall awareness and their attitudes towards these two forms of economic surveillance. H 1a is therefore not supported; a good part of users are concerned about economic surveillance on SNS (advertising and employer surveillance). Economic surveillance is visible to users.

Hypothesis 1b: A typical attitude expressed by SNS users is that they are concerned about job-related disadvantages in their working life caused by surveillance on SNS.

8 out of 30 interviewees mentioned surveillance by employers, when they were asked what they first link to the term of surveillance.

We are able to distinct between two dimensions in interviewees' attitudes towards employer surveillance: Cases who are worrying about employer surveillance and those who do not, on the one hand, and between those who dislike employer surveillance and those who find it OK, on the other hand. Along these dimensions, we found three attitudes: Those who find it OK and do not worry; those who dislike it but do not worry; and those who dislike it and worry about it. H 1b is therefore partly supported; we however found also unconcerned attitudes among SNS users.

Hypothesis 1c: The agreement respectively disagreement with certain kinds of surveillance depends on how much power students attribute to the particular entity that is watching.

In support of our hypothesis, nearly two third (19 interviewees), would only label top-down watching as problematic form of surveillance or privacy invasion, that is when professors watch their students on SNS. Lateral (students watch students) and

bottom-up watching (students watch their professors) is not perceived as problematic form of surveillance or privacy invasion by them. This, furthermore, supports the relevance of a critical theory of surveillance (Allmer 2012; Fuchs 2011f; 2012).

RQ1.2: Which role does a reference to privacy play in students' argumentation concerning communication on SNS? What do SNS users mean with "privacy"? What aspects of life should in the opinion of privacy-concerned SNS users remain private on SNS?

Our interviewees frequently named the privacy values freedom (9 times), including decisional freedom and freedom of opinion, and intimacy (10 times), including partnership, family and friendship. Privacy is most frequently valued because it ensures a realm where people can withdrawal to and find silence, regeneration, concentration, protection, time for (self-)reflection and thinking, and relief, for instance from others' evaluation, societal norms, or unwanted negative consequences (20 times). Less frequently, our interviewees argue that privacy enables impression management, that is the value to display different groups of people different aspects of the own identity (5 times), and has to do with trust (4 times) and respect (2 times). There is also substantial critique of the value of privacy.

Most frequently our interviewees argue that close relationships, such as the partner, family, or friends are typical private realms (14 times). The home is also an important private realm; interviewees speak in this context about the own four walls, and doors to close for instance (7 times). Sometimes interviewees mention financial and business information, such as the income, account balances, purchase information, client relations etc as private information (3 times). Ideology and the own thoughts, such as the political or religious perspective, as well as feelings or emotional problems, are also deemed to be private (each 3 times). More seldom in our sample people point to the body (2 times) and the nature (1 time) as private realms.

Our interviewees mentioned certain instances of the public interest that should set limits to privacy, such as ideas, knowledge, the educational sector, politics in general and politicians in particular, or, which was frequently mentioned, crimes.

When it comes to SNS we found clear individual notions of privacy among 13 interviewees. Further 11 interviewees are additionally concerned with youth protection. We interpret interviewees' exception from the individual privacy definition for non-adults users not as a typical inter-subjective privacy notion as their arguments for societal privacy definitions does not apply in general but to so to say imperfect individuals. In total 24 interviewees have then individualistic notions of privacy.

On the other hand, we found no clear social definitions of privacy. But we did find ambiguous, not clearly individual or inter-subjective/societal privacy notions among 6 interviewees.

Beside the context of SNS, we found in our interviewees' general reflections about the meaning of privacy aspects that point to a more inter-subjective or societal notion of privacy. Those aspects were that culture determines the notion of privacy, an equal

society would enable more privacy for all society members, privacy is determined by social norms and expectations, the common privacy notion should be the average of individual privacy needs, and privacy relies on the acceptance of others.

Hypothesis 2a: A reference to privacy is important in the argumentation of privacy-concerned SNS users against surveillance.

Before we asked privacy related questions, 20 out of 30 interviewees used the privacy term in their discussions of surveillance in general and of employer surveillance. After we picked up the privacy issue in the interviews, 16 interviewees argued that surveillance for targeted advertising affects users' privacy (the see that either clearly or were ambiguous). After the information input how advertising works on SNS, the number of those interviewees increased to 25. These results support the hypothesis that a reference to privacy is relevant in order to argue against surveillance on SNS.

Hypothesis 2b: SNS users typically express a view of privacy that is based on the control theory.

In respect to control and access theories of privacy, we found, contrary to our initial assumption that a trans-subjective notion of privacy is not necessarily linked to access theories; rather it is only one opportunity within this strand of theories. This modification became clear during our analysis of the interviews: Given the fact that most of our interviewees not only hold an individualistic notion of privacy but also define private realms, we assume that pure control theories do not explain the meaning of privacy for our interviewees appropriately. We are therefore not able support the hypothesis that users typically have privacy notions that are based on the control theory; rather we found that interviewees typically have individualistic notions of privacy.

Hypothesis 2c: SNS users typically express a view of privacy as an extrinsic value

During our interviews we recognised that in practice the debate about privacy as an intrinsic or extrinsic value is of less value as it is hard to differentiate between both justificatory ways and both ways do not strictly contradict each other. Privacy is a crucial, non-reducible value, but it is neither clearly intrinsic nor extrinsic. The result here is to reject H 2c and to reformulate that privacy is a non-reducible value for SNS users.

Hypothesis 2d: SNS users see privacy as private property

We related both categories, "attitudes towards selling personal data in exchange for money or 'premium options'" and "attitudes towards compensation payments to the users" and found that there are a notable number of 11 interviewees who disagree with both proposals. Those interviewees resist the ongoing "reconceptualization of privacy in the consumer's mind from a right or civil liberty to a commodity that can be exchanged for perceived benefits" (Campbell and Carlson 2002, 588; Comor 2011). On the other hand, we found a dominance of individual privacy notions that neglect societal/trans-subjective privacy definitions. Just as private property, so privacy be-

comes within these notions the right to exclude others. We found that users' privacy notions are frequently based on the control theory, which is characterised by subjective formalism. The indifference towards the content of privacy facilitates the individual alienation of privacy. We found evidence that property related information, such as financial or business information are deemed private by users. We also found concrete willingness to sell privacy among our interviewees, just like private property can be alienated. Furthermore we found in this context that some users are willing to receive an income for the usage of their private data (users want compensation for the usage of their data), just like it is recognised when it comes to the alienation of private property. We found that some users see privacy basically as inalienable persona right. However this position is not generally contradictory to a possessive individualistic notion of privacy as private property.

These results show that privacy may be seen as tradable commodity; if it is not then this may not automatically denote that privacy is not seen as private property. We found therefore support for H 2d.

RQ1.3: How do SNS users think about targeted advertising and alternative funding models? How do they relate this topic to privacy and surveillance issues?

Interestingly and unexpected 8 of 22 interviewees, who linked the economic aspect to the term of surveillance, named advertising as a form of economic surveillance. Obviously advertising – to a certain extend and for certain users – is visible as a form of surveillance. We found that the majority of our interviewees (18 out of 30) have a medium knowledge of how advertising works on SNS. These interviewees know that advertising on SNS is personalised or targeted but do not know more about how targeting works or hold wrong assumption about it. About 17 interviewees can be said that they have a fairly low awareness of the documents because they have at least witnessed changes in the documents but have not read them. The majority of the interviewees think that advertising influences the appearance or the functionalities of SNS at least in a way.

We were able to identify three influential lines of argumentation belonging to a positive attitude towards advertising on SNS (in total with 13 interviewees): First, interviewees say, that advertising and advertisements show no negative consequences for them because they are not forced to notice advertisements, to click on them, and to buy advertised products ultimately. Moreover, they are not forced to participate in SNS too. Second, interviewees made clear that advertisements on SNS show positive consequences for them, such as that they provide useful product information and interesting offers, and that it is fun watching them. The most important positive consequence indentified by the interviewees, however, was that advertising makes the usage of SNS free for them. Third, Interviewees agree with advertising on SNS as they find it a common and societal recognised funding model and because we all are used to have it.

We found four strands of arguments opposing advertising on SNS (in total with 10 interviewees). First, interviewees pointed to negative consequences of advertising for them. A particular strong expression of this strand is the argument that advertising on SNS is pressing, manipulating, and creates (unwanted) new needs. The most frequent negative consequences interviewees pointed to, are however weaker than manipulation and include annoyance and deflection. Second, interviewees frequently argue that advertising shows no positive consequences for them and that it is unnecessary and a waste of time. Third, interviewees argue that advertising contradicts SNS's inherent and real goal that is about maintaining and establishing social relations. Fourth, interviewees lament that there is no alternative to this funding model.

Hypothesis 3a: SNS users typically argue that they do not see targeted advertising as a privacy threat and not as a problematic form of surveillance.

15 Interviewees said that targeted advertising is not problematic and not affecting their privacy invasively, 11 interviewees said that it is a privacy invasion or a problematic form of surveillance, 4 interviewees remain ambiguous.

Those who neglect targeted advertising as a problematic form of surveillance or a privacy invasion could be easily and clearly grouped into two major strands of argumentation: First, it was argued that there was an informed consent by the user to the SNS's terms of use, which also includes the acceptance of targeted advertising. Second, similarly to one strand of agreement listed above, it was pointed out that advertising on SNS shows no negative consequences for users. The particular argument in this context is that one cannot be identified by third parties (any actor outside the relationship between user and SNS provider).

Those who think that targeted advertising is a problematic form of surveillance or a privacy invasion, employed the following strands of arguments (here again in parts, arguments oppose to the neglecting ones diametrically). First, interviewees challenge that there was an informed consent to advertising. Interviewees secondly argued (referring to direct consequences) that advertising on SNS is a problematic form of surveillance as it is too excessively and disproportionally performed by the SNS provider. Third, interviewees argue, that advertising on SNS shows indirect consequences because the data collected for this purpose can be accessed by third parties, such as state authorities or hackers, later on. Fourth, interviewees are uncertain about the exact use of their data and this uncertainty is linked to potential consequences for them.

After the information input about targeted advertising works on SNS, we could observe a significant number of interviewees who switched to a negative perception of advertising. They see it now as a problematic form of surveillance or a privacy invasion, or, in two cases, as they have already perceived it as a privacy invasion they switched from agreement to disagreement with advertising on SNS.

The overall significance of changes after the information input let us assume that the degree of users' knowledge and awareness of economic surveillance plays a key role in influencing the perception whether it is problematic or a privacy invasion.

Hence the assumption that there is an informed consent becomes quite questionable and many users would not agree with advertising on SNS if they knew how it exactly works. In terms of H 3a, we are not able to either support or reject it. We suggest to formulate that informed SNS users will perceive targeted advertising as a privacy threat.

Hypothesis 3b: SNS users say that public funding of SNS is a better option than advertising-financing. Those who express doubts argue that public funding or alternative funding strategies (like donation models) tend to be inefficient and ineffective.

A potential public funding model for SNS gains least support in comparison to traditional pay per use, and donation funding. Frequent arguments why interviewees challenge a public funding model for SNS are: First, not everyone uses SNS but the costs have to be afforded by all. Second, interviewees argue that there is no public interest in providing SNS, they already exists without public funding. Obviously the specific (for instance, alienated or exploitative) quality of the SNS does not play a role within this arguments. Given the fact that non-commercial alternative SNS are unknown, this applies in particular. Third, users argue that the state would then influence SNS and should therefore not organise the funding of SNS. The state appears as the only entity that is able to do public funding. On the other hand, those interviewees who support a public funding model apply the following lines of argumentation: First, there is a real public interest: SNS are used by so many and public funding would effectively save costs for society because the costs will be less than the total costs generated by advertising. Second, public funding could help to close digital divides and would avoid exclusion, for instance through social sorting. Third, public funding would enable to make mandatory requirements for SNS, such as better terms of use for instance. Fourth, those who are critical about commercial SNS argue that a public funding model would ensure that SNS become non-commercial.

It is salient that all interviewees express a supportive attitude towards introduced alternative SNS, which make use of alternative funding models. We were able to differentiate between two forms of user support, one is support in a non-material way and one is monetary support. Whereas all interviewees support alternative SNS at least ideally, the half of our sample (15 out of 30) replied our question whether they would also support alternatives monetarily with a positive statement. If only one percent of the one billion Facebook users would switch to an alternative SNS and support it with 5 Euros a year, this alternative SNS would be equipped with 50 million Euros a year.

In terms of H 3b, we are able to assess that users prefer the non-capitalist funding strategy that is based on donations.

RQ1.4: Do students think that there is a privacy-user benefit trade-off on SNS? Why respectively why not? In this context, which arguments do they employ to argue for privacy and against surveillance on SNS? Which arguments do they employ to argue for surveillance and against privacy on SNS?

Users think that there is a privacy-user benefit trade-off. The strategy of limited disclosure is the most influential among our interviewees (19 interviewees applied it) and helps them reaching a point where they say that the benefits of SNS outweigh the surveillance and privacy threats clearly.

According to our critical theoretical approach, we are also interested in aspects of alienation on SNS. Can aspects of alienation be found on SNS? We found some evidence of it in the (limited range of) trade-off strategies that users usually employ when they participate in SNS. Also interesting in this context is that interviewees shared several reflexions about the conditions of their trade-off strategies with us. Besides, pointing to the dynamic nature of their trade-offs (that their trade-offs will change when their life situation changes, that the positive outcome of the trade-off is quite fragile, and that negative publicity will alter the trade-off), a third of our sample argues that there is a kind of heteronomy (no informed consent to the terms of use and privacy policies, limited spectrum of possible decision they can make when they use SNS)

It is salient from our material that interviewees have more points of critique towards the terms of use and privacy policy than they have according the overall privacy protection through the SNS provider. The influential arguments about the intransparency of how and if privacy can be protected refers to deficient privacy policies and the terms of use.

Users make the following suggestions about points that should be included to the terms of use and privacy policies of SNS: SNS should ensure that there is a informed consent to changes on the SNS; they wish a deleting of data after a certain period of time or of old data after changes were made; they suggest that the SNS does no statistical analysis of the users' data; the SNS should not disclose data to third parties, in particular it should not sell user data; personal data should not appear elsewhere than on the genuine site; user should remain perfect ownership of uploaded data; they wish clear and concise terms of use and privacy policies; they further suggest traditional instead of targeted advertisements; and that the SNS makes no own suggestions of potential friends to users; finally, that the SNS should not perform face recognition of its users.

The most important suggestion is the introduction of an opt-in opportunity for advertising on SNS. The results in this context are that only one out of 30 interviewees does not want the opportunity to enable first, before data can be used for advertising. The overwhelming majority would even welcome a law which makes opt-in for advertising mandatory. The introduction of an opt-in opportunity for advertising, which is highly wanted by our interviewees, would seriously question SNS that are profit oriented. It is likely that a significant number of users will disable advertising if they had the opportunity to do so.

6. The study at hand in the context of the other studies conducted in the research project

Allmer (2012) conducted a quantitative online survey among the Austrian student population that focuses on the greatest (dis-)advantages that students see when using SNS and explores their notion of privacy. The distribution of SNS usage according different SNS that was found by Allmer (2012, 30) justifies our focus on the leading SNS, Facebook in the qualitative study at hand. Allmer (2012, 31-39) lists the main advantages for using SNS that users see. These information complement to understand our discussion of privacy-user benefit trade-offs (see section 4.1.5). Among the greatest disadvantages users see the surveillance and privacy problems (Allmer 2012, 39-41) which shows that privacy-user benefits trade-offs is an important field of study. Allmer was able to detect in his study a weak predominance of an intrinsic privacy value concept among students. He used quantifying means ("privacy value index"; Allmer 2012, 50-51) to come to this result. The study at hand is qualitative and found that privacy is seen both as intrinsic and extrinsic. Given that in Allmer's study most of the students do not have clear intrinsic or extrinsic understandings of the privacy value but see privacy "rather" as intrinsic or extrinsic value means that Allmer's results do not contradict our results in principle. Allmer's results concerning privacy theories (control or access) and his "privacy theory index"; Allmer 2012, 58-59) are based on an interpretation of the control theory as individualistic and the access theory as societal. Indeed this was the initial understanding also within the study at hand. However we found then that these identifications are misleading and were able to provide evidence that access theories of privacy need not be social but can be individualistic. We consequently focused in our study on the differentiation between social and individual notions of privacy rather than the differentiation between control and access privacy notions.

Kreilinger (2013) also conducted a quantitative online survey among the Austrian student population but focused on knowledge, attitudes, and information behaviour in the context of surveillance and privacy issues. Targeted advertising as a form of economic surveillance gained particular attention in Kreilinger's study, which can be therefore sees as a valuable complementary perspective to our study. Kreilinger, like the study at hand, found out that users have low or wrong knowledge about advertising on SNS and the respective content of the terms of use and privacy policies. Kreilinger found that there is a significant positive relationship between users who are more concerned about their privacy and respondents who are against targeted advertising. Our results offer insights in users' lines of argumentation and show why or why not users see targeted advertising on SNs as a privacy invasion. Comparing knowledge, attitudes and behaviour Kreilinger's study found some contradictions between what users say and what they actually do. Research on user behaviour, as Kreilinger did, is a meaningful complementation to the interview study at hand.

7. Limitations of the study and suggestions for further research

We assumed that "privacy invasion" and a "problematic form of surveillance" have the same meaning for SNS users. However, that is not a necessity. There are convincing arguments that privacy is not the right term to oppose surveillance as it frames structural problems in individual terms (e.g. Stalder 2002); it would be interesting to systematically explore the relationship between privacy and surveillance in detail and whether both terms have different meanings for SNS user. We tried to handle this problem by using the expression "problematic form of surveillance" in our interviews. That surveillance is primarily seen as a negative term was one of the results of our study.

A second limitation is more general, but links to the previous one insofar as surveillance is thought of as mere structural category than privacy. Critical theory assumes a gap between the objective existence of alienation and exploitation in society and their subjective perception, although we tried to find evidence for both in our interviews, the method of interviewing faces limitations to study objectified structures. Further research should engage in thinking about alternative methods to approach exploitation, immaterial labour, and alienation on SNS. It would be interesting to study these crucial issues separately and hence in more detail.

Sometimes it became difficult to differentiate between interviewees' own attitudes and interviewees' description of a status quo. The problem of distinction between "there is" and "there should be" appears in particular when we spoke about the privacy notion with our interviewees. We tend to identify interviewee's descriptions with their attitudes.

References

Acquisti, Allessandro, and Ralph Gross. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook." In Proceedings of 6th Workshop on Privacy Enhancing Technologies, ed. Phillipe Golle and George Danezis. Camebridge, UK: Robinson College.

Adorno, Theodor W. 1976a. "On the Logic of the Social Sciences." In The Positivist Dispute in German Sociology, ed. Theodor W. Adorno, Hans Albert, Ralf Dahrendorf, Jürgen Habermas, Harald Pilot, and Karl R. Popper, 105–122. London: Heinemann.

———. 1976b. "Sociology and Empirical Research." In The Positivist Dispute in German Sociology, ed. Theodor W. Adorno, Hans Albert, Ralf Dahrendorf, Jürgen Habermas, Harald Pilot, and Karl R. Popper, 68–86. London: Heinemann.

———. 1976c. "Introduction." In The Positivist Dispute in German Sociology, ed. Theodor W. Adorno, Hans Albert, Ralf Dahrendorf, Jürgen Habermas, Harald Pilot, and Karl R. Popper, 1–67. London: Heinemann.

Adorno, Theodor W., Hans Albert, Ralf Dahrendorf, Jürgen Habermas, Harald Pilot, and Karl R. Popper. 1976. The Positivist Dispute in German Sociology. London: Heinemann.

Albrechtslund, Anders. 2008. "Online Social Networking Sites and Participatory Surveillance." First Monday 13 (3). http://firstmonday.org/article/view/2142/1949.

Albrechtslund, Anders, and Lynsey Dubbeld. 2005. "The Plays and Arts of Surveillance: Studying Surveillance as Entertainment." Surveillance & Society 3 (2/3): 216–221.

Allen, Anita. 1988. Uneasy Access. Totowa: Rowman & Littlefield.

Allmer, Thomas. 2011. "A Critical Contribution to Theoretical Foundations of Privacy Studies." Journal of Information, Communication and Ethics in Society 9 (2): 81–101.

———. 2012. Towards a Critical Theory of Surveillance in Informational Capitalism. Frankfurt am Main: Peter Lang.

———. 2012. "Research Design & Data Analysis, Presentation, and Interpretation: Part One (SNS3 Research Paper Number 12)". UTI.

Altman, Irwin. 1976. "Privacy. A Conceptual Analysis." In Environment and Behavior 8 (1): 7–29.

Andrejevic, Mark. 2002. "The Work of Being Watched: Interactive Media and the Exploration of Self-Disclosure." Critical Studies in Media Communication 19 (2) (June): 231. doi:Article.

———. 2004. Reality TV: The Work of Being Watched. Lanham: Rowman & Littlefield Publishers. internal-pdf://0742527484-3909742080/0742527484.pdf.

———. 2005. "The Work of Watching One Another: Lateral Surveillance, Risk, and Governance." Surveillance & Society 2 (4): 479–497.

———. 2010. "Social Network Exploitation." In A Networked Self: Identity, Community, and Culture on Social Networking Sites, ed. Zizi Papacharisi, 82–101. New York; London: Routledge.

———. 2011. "Surveillance and Alienation in the Online Economy." Surveillance & Society 8 (3): 278–287.

———. 2012. "Exploitation in the Data Mine." In Internet and Surveillance: The Challenges of Web 2.0 and Social Media, ed. Christian Fuchs, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval, 71–88. New York: Routledge.

Arber, Sara. 1993. "Designing Samples." In Researching Social Life, ed. Nigel Gilbert, 68–92. London; Thousand Oaks; New Dehli: Sage.

Babbie, Earl. 2010. The Practice of Social Research. Belmont: Wadsworth.

Barnes, Susan. 2006. "A Privacy Paradox: Social Networking in the United States." First Monday 11 (9).

http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312.

Barter, Christine, and Emma Renold. 1999. "The Use of Vignettes in Qualitative Research." Social Research Update 25. http://sru.soc.surrey.ac.uk/SRU25.html.

Beer, David. 2008. "Social Network(ing) Sites ... Revisiting the Story so Far: A Response to Danah Boyd & Nicole Ellison." Journal of Computer-Mediated Communication 13 (2): 516–529.

Bennett, Colin, and Charles Raab. 2006. The Governance of Privacy: Policy Instruments in Global Perspective. [2. and updated ed.]. Cambridge, MA: MIT Press.

Bosau, C, O Fischer, and M Koll. 2008. "StudiVZ: Determinants of Social Networking and Dissemination of Information Among Students." In Berlin.

Boutang, Vann Moulier. 2012. Cognitive Capitalism. Cambridge: Polity.

Boyd, Danah, and Eszter Hargittai. 2010. "Facebook Privacy Settings: Who Cares?" First Monday 15 (8). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589.

Brenkert, George G. 1979. "Freedom and Private Property in Marx." Philosophy and Public Affairs 8 (2): 122–147.

Bruns, Axel. 2008. Blogs, Wikipedia, Second Life, and Beyond: From Production to Produsage. New York: Peter Lang.

Burawoy, Michael. 1998. "The Extended Case Method." Sociological Theory 16 (1): 4–33.

Campbell, John Edward, and Matt Carlson. 2002. "Panopticon.com: Online Surveillance and the Commodification of Privacy." Journal of Broadcasting & Electronic Media 46 (4): 586. doi:Article.

Chan, Yolande E., L. Lynda Harling Stalker, and David Lyon. 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:10.1089/cpb.2008.0226.

Comor, Edward. 2010. "Digital Prosumption and Alienation." Ephemera: Theory & Politics in Organization 10 (3/4): 439–454.

Culnan, Mary J., and Pamela K. Armstrong. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation." Organization Science 10 (1): 104–115.

Debatin, Bernhard, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes. 2009. "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Con-

sequences." Journal of Computer-Mediated Communication 15 (1): 83–108. doi:10.1111/j.1083-6101.2009.01494.x.

Dennis, Kingsley. 2008. "Keeping a Close Watch: The Rise of Self-surveillance and the Threat of Digital Exposure." Sociological Review 56 (3): 347–357.

van Dijk, Niels. 2010. "Property, Privacy and Personhood in a World of Ambient Intelligence." Ethics and Information Technology 12 (1): 57–69.

Dwyer, Catharine, Starr Hiltz, Marshall Poole, Julia Gussner, Felicitas Hennig, Sebastian Osswald, Sandra Schliesslberger, and Birgit Warth. 2010. "Developing Reliable Measures of Privacy Management Within Social Networking Sites." In Proceedings of the 43rd Hawaii International Conference on System Sciences, 2968–2977. Los Alamitos: IEEE Computer Society.

Dwyer, Catharine, Katia Passerini, and Starr Roxanne Hiltz. 2007. "Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace." In Proceedings of the Thirteenth Americas Conference on Information Systems. Keystone, Colorado.

Dyer-Witheford, Nick. 2010. "Digital Labour, Species-becoming and the Global Worker." Ephemera: Theory & Politics in Organization 10 (3/4): 484–503.

Ekos. 2004. "Globalization of Personal Data Project: International Survey: Findings from the Pre-survey Focus Groups." http://www.sscqueens.org/sites/default/files/Canada_FG_Findings_Ekos_May_2004.pdf.

Ellison, Nicole B., Charles Steinfield, and Cliff Lampe. 2007. "The Benefits of Facebook 'Friends:' Social Capital and College Students' Use of Online Social Network Sites." Journal of Computer-Mediated Communication 12 (4): 1143–1168. doi:10.1111/j.1083-6101.2007.00367.x.

Ellison, Nicole B., Jessica Vitak, Charles Steinfield, Rebecca Gray, and Cliff Lampe. 2011. "Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment." In Privacy Online: Perspectives on Privacy and Self-disclosure in the Social Web, ed. Sabine Trepte and Leonard Reinecke, 19–32. Berlin: Springer.

Etzioni, Amitai. 1999. The Limits of Privacy. New York, NY: Basic Books.

———. 2005. "The Limits of Privacy." In Contemporary Debates in Applied Ethics, ed. Andrew I. Cohen and Christopher Heath Wellman, 253–262. Malden, MA: Blackwell.

Fay, Brian. 1993. "The Elements of Critical Social Science." In Social Research: Philosophy, Politics, and Practice, ed. Martyn Hammersley, 33–36. London; Thousand Oaks; New Dehli: Sage.

Fernback, Jan, and Zizi Papacharisi. 2007. "Online Privacy as Legal Safeguard: The Relationship Among Consumer, Online Portal, and Privacy Policies." New Media & Society 9 (5): 715–734.

Fielding, Jane. 1993. “Coding and Managing Data.” In Researching Social Life, ed. Nigel Gilbert. London; Thousand Oaks; New Dehli: Sage.

Fielding, Nigel. 1993. “Qualitative Interviewing.” In Researching Social Life, ed. Nigel Gilbert, 135–153. London; Thousand Oaks; New Dehli: Sage.

Finch, Janet. 1987. “The Vignette Technique in Survey Research.” Sociology 21 (1): 105–114.

Fisher, Eran. 2012. “How Less Alienation Creates More Exploitation? Audience Labour on Social Network Sites.” tripleC: Journal for a Sustainable Information Society 10 (2): 171–183.

Foddy, William. 1993. Constructing Questions for Interviews and Questionnaires: Theory and Practice in Social Research. Camebridge: Cambridge University Press.

Fogel, Joshua, and Elham Nehmad. 2009. “Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns.” Computers in Human Behavior 25 (1): 153–160. doi:10.1016/j.chb.2008.08.006.

Fontana, Andrea, and James H. Frey. 2005. “The Interview: From Neutral Stance to Political Involvement.” In The Sage Handbook of Qualitative Research, ed. Norman K. Denzin and Norman Lincoln, 695–727. London; Thousand Oaks; New Dehli: Sage.

Foucault, Michel. 1977. Discipline and Punish: The Birth of the Prison. New York: Vintage Books.

Fried, Charles. 1970. An Anatomy of Values. Cambridge: Harvard University Press.

———. 1984. “Privacy.” In Philosophical Dimensions of Privacy: An Anthology, ed. Ferdinand Schoeman, 203–222. Camebridge: Cambridge University Press.

Froomkin, A. Michael. 2000. “The Death of Privacy?” Stanford Law Review 52 (5): 1461–1543.

Fuchs, Christian. 2008. Internet and Society: Social Theory in the Information Age. New York: Routledge.

———. 2010a. “studiVZ: Social Networking in the Surveillance Society.” Ethics and Information Technology 12 (2): 171–185.

———. 2010b. “Labour in Informational Capitalism.” The Information Society 26 (3): 176–196.

———. 2010c. “Class, Knowledge and New Media.” Media, Culture and Society 32 (1): 141–150.

———. 2011a. “The Political Economy of Privacy.” The Internet & Surveillance - Research Paper Series 8. http://www.sns3.uti.at.

———. 2011b. “An Alternative View of Privacy on Facebook.” Information 2: 140–165. doi:10.3390/info2010140.

———. 2011c. “Web 2.0, Prosumption, and Surveillance.” Surveillance & Society 8 (3): 288–309.

———. 2011d. “New Media, Web 2.0 and Surveillance.” Sociological Compass 5: 134–147.

———. 2011e. “Towards an Alternative Concept of Privacy.” Journal of Information, Communication and Ethics in Society 9 (4): 220–237.

———. 2011f. “How to Define Surveillance?” MATRIZes 5 (1): 109–133.

———. 2012. “Critique of the Political Economy of Web 2.0 Surveillance.” In Internet and Surveillance: The Challenges of Web 2.0 and Social Media, ed. Christian Fuchs, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval, 31–70. New York: Routledge.

Gandy, Oscar H. 1993. The Panoptic Sort: A Political Economy of Personal Information. Boulder: Westview Press.

———. 2003. “Public Opinion Surveys and the Formation of Privacy Policy.” Journal of Social Issues 59 (2): 283–299.

Gavinson, Ruth. 1980. “Privacy and the Limits of Law.” Yale Law Journal 89 (1): 421–471.

Geuss, Raymond. 2001. Public Goods, Private Goods. Princeton, NJ: Princeton University Press.

Gilliom, John. 2001. Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy. Chicago, IL: University of Chicago Press.

Goldring, John. 1984. “Privacy and Property.” The Australien Quarterly 56 (4): 308–324.

Gorelick, Sherry. 1991. “Contradictions of Feminist Methodology.” Gender & Society 5 (4): 459–477. doi:10.1177/089124391005004002.

Habermas, Jürgen. 1991. The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society. Cambridge, MA: MIT Press.

Haggerty, Kevin D., and Richard V. Ericson. “The Surveillant Assemblage.” British Journal of Sociology 51 (4): 605–622.

Hardt, Michael, and Antonio Negri. 2004. Multitude: War and Democracy in the Age of Empire. New York: Penguin.

Haug, Wolfgang Fritz. 1986. Critique of Commodity Aesthetics: Appearance, Sexuality, and Advertising in Capitalist Society. Minneapolis, MN: University of Minnesota Press.

———. 2005. Vorlesungen Zur Einführung Ins “Kapital”. Berlin: Argument.

———. 2006. “Commodity Aesthetics Revisited: Exchange Relations as the Source of Antagonistic Aesthetization.” Radical Philosophy 135: 18–24.

Hettinger, Edwin C. 1989. “Justifiying Intellectual Property.” Philosophy and Public Affairs 18 (1): 31–52.

Horkheimer, Max. 2002. “Traditional and Critical Theory.” In Critical Theory: Selected Essays, 188–243. New York: Continuum.

Jhally, Sut. 1990. The Codes of Advertising: Fetishism and the Political Economy of Meaning in Consumer Society. New York: Routledge.

Jhally, Sut, and Bill Livant. 1986. “Watching as Working: The Valorisazion of Audience Consciousness.” Journal of Communication 36 (3): 124–143.

Kang, Jerry. 1998. “Information Privacy in Cyberspace Transactions.” Stanford Law Review 50: 1193–1294.

Kincheloe, Joe L., and Peter McLaren. 2005. “Rethinking Critical Theory and Qualitative Research.” In The Sage Handbook of Qualitative Research, ed. Norman K. Denzin and Norman Lincoln, 303–342. London; Thousand Oaks; New Dehli: Sage.

Knoche, Manfred. 2003. “Freie Radios - Frei Von Staat, Markt Und Kapital(ismus)? Zur Widersprüchlichkeit Alternativer Medien Und Ökonomie.” Medien Journal 27 (4): 4–19.

Kolakowski, Leszek. 1993. “An Overall View of Positivsm.” In Social Research: Philosophy, Politics, and Practice, ed. Martyn Hammersley, 1–8. London; Thousand Oaks; New Dehli: Sage.

Koskela, Hille. 2004. “Webcams, TV Shows and Mobile Phones: Empowering Exhibitionism.” Surveillance & Society 2 (2/3): 199–215.

Kowal, Sabine, and Daniel O’Connell. 2004. “The Transcription of Conversations.” In A Companion to Qualitative Research, ed. Uwe Flick, Ernst von Kardorff, and Ines Steinke, 248–252. London; Thousand Oaks; New Dehli: Sage.

Kracauer, Siegfried. 1952. “The Challenge of Qualitative Content Analysis.” The Public Opinion Quarterly 16 (4): 631–642.

Kreilinger, Verena. 2013. “Research Design & Data Analysis, Presentation, and Interpretation: Part Two (SNS3 Research Paper Number 13)”. UTI.

Kuckartz, Udo. 2010. Einführung in Die Computergestützte Analyse Qualitativer Daten. Wiesbaden: VS Verlag für Sozialwissenschaften.

Kvale, Steinar. 2007. Doing Interviews. London; Thousand Oaks; New Dehli: Sage.

Lange, Patricia. 2007. “Publicly Private and Privately Public: Social Networking on YouTube.” Journal of Computer Mediated Communication 13 (1). http://jcmc.indiana.edu/vol13/issue1/lange.html.

Laudon, Kenneth C. 1996. “Markets and Privacy.” Communications of the ACM 39 (9): 92–104.

Lazzarato, Maurizio. 1996. “Immaterial Labor.” In Radical Thought in Italy: A Potential Politics, ed. Paolo Virno and Michael Hardt, 133–148. Minneapolis: University of Minnesota Press.

Lenhart, Amanda, and Mary Madden. 2007. PEW Internet & Amercian Life Project: Social Networking Websites and Teens: An Overview.

Lessig, Lawrence. 2002. "Privacy as Property." Social Research 69 (1): 247–269.

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): 79–100. doi:10.1111/j.1083-6101.2008.01432.x.

Litman, Jessica. 2000. "Information Privacy/Information Property." Stanford Law Review 52 (5): 1283–1313.

Livingstone, Sonia. 2008. "Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy and Self-expression." New Media & Society 10 (3): 393–411.

Lyon, David. 1994. The Electronic Eye: The Rise of Surveillance Society. Minneapolis, MN: University of Minnesota Press.

———. 2005. Surveillance Society: Monitoring Everyday Life. Buckingham: Open University Press.

———. 2007. Surveillance Studies: An Overview. Cambridge; Malden, MA: Polity.

Macpherson, C. 1962. The Political Theory of Possessive Individualism: Hobbes to Locke. Oxford: Clarendon Press.

Macpherson, Crawford B. 1978a. "Liberal-democracy and Property." In Property: Mainstream and Critical Positions, ed. Crawford B. Macpherson, 199–207. Toronto, ON: University of Toronto Press.

———. 1978b. "The Meaning of Property." In Property: Mainstream and Critical Positions, ed. Crawford B. Macpherson, 1–13. Toronto, ON: University of Toronto Press.

Mann, Steven, Jason Nolan, and Barry Wellman. 2003. "Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments." Surveillance & Society 1 (3): 331–355.

Marx, Karl. 1867. Capital: A Critique of Political Economy: Volume One. Middlesex: Penguin.

———. 1972a. "On the Jewish Question." In Writings of the Young Marx on Philosophy and Society, 216–248. Indianapolis: Hackett.

———. 1972b. The Eigtheenth Brumaire of Louis Bonaparte. Moscow: Progress Publishers.

———. 1988. "Economic and Philosophic Manuscripts of 1844." In Economic and Philosophic Manuscripts of 1844 and the Communist Manifesto, 13–168. Amherst: Prometheus.

Mathiesen, Thomas. 1997. "The Viewer Society: Michel Foucault's 'panopticon' Revisited." Theoretical Criminology 1 (2): 215–234.

———. 2004. “Panopticon and Synopticon as Silencing Systems.” In Silently Silenced. Essays on the Creation of Acquiesence in Modern Society, 98–102. Winchester:: Waterside Press.

Mayring, Philipp. 2004. “Qualitative Content Analysis.” In A Companion to Qualitative Research, ed. Uwe Flick, Ernst von Kardorff, and Ines Steinke, 266–269. London; Thousand Oaks; New Dehli: Sage.

McLellan, David, ed. 2000. Karl Marx: Selected Writings. Oxford: Oxford University Press.

Mies, Maria. 1993. “Towards a Methodology of Feminist Research.” In Social Research: Philosophy, Politics, and Practice, ed. Martyn Hammersley, 64–82. London; Thousand Oaks; New Dehli: Sage.

Miles, Matthew B., and A. Michael Huberman. 1994. Qualitative Data Analysis. London; Thousand Oaks; New Dehli: Sage.

Mill, John Stuart. 1965. Principles of Political Economy. London: University of Toronto Press.

Miller, Arthur R. 1971. The Assault on Privacy. Cambridge, MA: Harvard University Press.

Moor, James H. 1997. “Towards a Theory of Privacy in the Information Age.” Computers and Society 27 (3): 27–32.

Moore, Adam D. 2008. “Defining Privacy.” Journal of Social Philosophy 39 (3): 411–428.

Munzer, Stephen R. 2005. “Property.” In The Shorter Routledge Encyclopedia of Philosophy, ed. Edward Craig, 858–861. London; New York: Routledge.

Newell, Rosemarie. 1993. “Questionnaires.” In Researching Social Life, ed. Nigel Gilbert, 94–115. London; Thousand Oaks; New Dehli: Sage.

Nissenbaum, Helen. 2010. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, CA: Stanford Law Books.

Nock, Steven. 1993. The Costs of Privacy: Surveillance and Reputation in America. New York: de Gruyter.

Norberg, Patricia, Daniel R. Horne, and David A. Horne. 2007. “The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors.” Journal of Consumer Affairs 41 (1): 100–126.

Nowak, Glen J., and Joseph E. Phelps. 1992. “Understanding Privacy Concerns: An Assessment of Consumers’ Information-related Knowledge and Beliefs.” Journal of Direct Marketing 6 (4): 28–39. doi:10.1002/dir.4000060407.

Ogura, Toshimaru. 2006. “Electronic Government and Surveillance-oriented Society.” In Theorizing Surveillance: The Panopticon and Beyond, ed. David Lyon, 270–295. Portland: Willan.

Pasquinelli, Matteo. 2009. Animal Spirits: A Bestiary of the Commons. Rotterdam: NAi Publishers.

Pateman, Carole. 2002. "Self-ownership and Property in the Person: Democratization and a Tale of Two Concepts." Journal of Political Philosophy 10 (1): 20–53.

Punch, Keith F. 2005. Introduction to Social Research: Quantitative and Qualitative Approaches. London: Sage.

Quinn, Michael J. 2006. Ethics for the Information Age. Boston: Pearson.

Rachels, James. 1975. "Why Privacy Is Important." Philosophy and Public Affairs 4 (4): 323–333.

Reiman, Jeffrey. 1976. "Privacy, Intimacy, and Personhood." Philosophy and Public Affairs 6 (1): 22–44.

Reinharz, Shulamit. 1992. Feminist Methods in Social Research. Oxford; New York: Oxford University Press.

Rey, P J. 2012. "Alienation, Exploitation, and Social Media." American Behavioral Scientist 56 (4): 399–420.

Ritsert, Jürgen. 1972. Inhaltsanalyse Und Ideologiekritik: Ein Versuch Über Kritische Sozialforschung. Frankfurt am Main: Athenäum Fischer.

Rössler, Beate. 2001. Der Wert Des Privaten. Frankfurt am Main: Suhrkamp.

Samuelson, Pamela. 2000. "Privacy as Intellectual Property?" Stanford Law Review 52 (5): 1125–1173.

Sandoval, Marisol. 2009. "A Critical Contribution to the Foundation of Alternative Media Studies." Kurgu. Online International Journal of Communcation Studies (1). http://www.kurgu.anadolu.edu.tr/dosyalar/6.pdf.

———. 2011. "A Critical Empirical Case Study of Consumer Surveillance on Web 2.0." In Internet and Surveillance: The Challenge of Web 2.0 and Social Media, ed. Christian Fuchs, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval. New York: Routledge.

Sandoval, Marisol, and Christian Fuchs. 2010. "Towards a Critical Theory of Alternative Media." Telematics and Informatics 27: 141–150.

Schmidt, Christiane. 2004. "The Analysis of Semi-structured Interviews." In A Companion to Qualitative Research, ed. Uwe Flick, Ernst von Kardorff, and Ines Steinke, 253–258. London; Thousand Oaks; New Dehli: Sage.

Schoeman, Ferdinand. 1984. Philosophical Dimensions of Privacy: An Anthology. Cambridge; New York: Cambridge University Press.

Schwartz, Barry. 1968. "The Social Psychology of Privacy." American Journal of Sociology 73 (6): 741–752.

Sevignani, Sebastian. 2011. "A Contribution to Foundations of a Critical Theory of Privacy (SNS3 Research Paper Number 7)". UTI.

———. 2012. “The Problem of Privacy in Capitalism and the Alternative Social Networking Site Diasproa*.” tripleC: Journal for a Sustainable Information Society (special Issue Marx Is Back-The Importance of Marxist Theory and Research for Critical Comm. Studies Today, Ed C. Fuchs & Vincent Mosco) 10 (2): 600–617.

Sevignani, Sebastian, Verena Kreilinger, Thomas Allmer, and Christian Fuchs. 2011. “Analysis of Existing Empirical Research Methods for Studying (online) Privacy and Surveillance”. Unified Theory of Information Research Group. http://www.sns3.uti.at/wp-content/uploads/2010/09/The-Internet-and-Surveillance-Research-Paper-Series-No.10_-Analysis-of-Existing-Empirical-Research-Methods-for-Studying-Privacy-and-Surveillance.pdf.

Sheehan, Kim. “Toward a Typology of Internet Users and Online Privacy Concerns.” The Information Society 18 (1): 21–32.

Shepherd, Tamara. 2012. “Persona Rights for User-generated Content: A Normative Framework for Privacy and Intellectual Property Regulation.” tripleC 10 (1): 100–113.

Shils, Edward. 1966. “Privacy: Its Constitution and Vicissitudes.” Law & Contemporary Problems 31 (2): 281–306.

Smythe, Dallas W. 2006. “On the Audience Commodity and Its Work.” In Media and Cultural Studies: Keyworks, ed. Durham G. Meenakshi and Douglas Kellner, 230–256. Malden, MA: Blackwell.

Sofsky, Wolfgang. 2007. Verteidigung Des Privaten: Eine Streitschrift. München: C. H. Beck.

Solove, Daniel J. 2009. Understanding Privacy. Camebridge, MA; London, UK: Harvard University Press.

Spinello, Richard. 2006. CyberEthics: Morality and Law in Cyberspace. Sudbury, MA: Jones and Bartlett.

Stalder, Felix. 2002. “Opinion: Privacy Is Not the Antidote to Surveillance.” Surveillance & Society 1 (1): 120–124.

Tavani, Herman T. 2008. “Informational Privacy: Concepts, Theories, and Controversies.” In The Handbook of Information and Computer Ethics, ed. Kenneth Einar Himma and Tavani, 131–164. Hoboken, NJ: Wiley.

Terranova, Tiziana. 2000. “Free Labour: Producing Culture for the Digital Economy.” Social Texts 18 (2): 33–58.

Tufekci, Zynep. 2008. “Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites.” Bulletin of Science, Technology & Society 28 (1): 20–36.

Turow, Joseph, and Michael Hennessy. 2007. “Internet Privacy and Institutional Trust.” New Media & Society 9 (2): 300–318.

Turow, Joseph, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy. Contrary to What Marketers Say, Americans Reject Tailored Advertising: And Three Activities That Enable It. University of Pennsylvania and Berkeley Center for Law & Technology.

Utz, Sonja, and Nicole C. Krämer. 2009. "The Privacy Paradox on Social Network Sites Revisited: The Role of Individual Characteristics and Group Norms." Cyberpsychology: Journal of Psychosocial Research on Cyberspace 3 (2): 1–11.

Varian, Hal R. 1997. "Economic Aspects of Personal Privacy." In Privacy and Self-regulation in the Information Age, ed. National Telecommunications and Information Administration (NTIA). Washington: NTIA.

Wacks, Raymond. 2010. Privacy. A Very Short Introduction. Oxford: Oxford University Press.

Wang, Paul, and Lisa A. Petrison. 1993. "Direct Marketing Activities and Personal Privacy: a Consumer Survey." Journal of Direct Marketing 7 (1): 7–19.

Ward Schofield, Janet. 1993. "Increasing the Generalizability of Qualitative Research." In Social Research: Philosophy, Politics, and Practice, ed. Martyn Hammersley, 200–225. London; Thousand Oaks; New Dehli: Sage.

Warren, Samuel, and Louis Brandeis. 1890. "The Right to Privacy." Harvard Law Review 4 (5): 193–220.

Westin, Alan. 1967. Privacy and Freedom. New York, NY: Atheneum.

Zywica, Jolene, and James Danowski. 2008. "The Faces of Facebookers: Investigating Social Enhancement and Social Compensation Hypotheses; Predicting Facebook and Offline Popularity from Sociability and Self-esteem, and Mapping the Meanings of Popularity with Semantic Networks." Journal of Computer-Mediated Communication 14: 1–34.