

CHRISTIAN FUCHS

SOCIAL NETWORKING SITES AND THE SURVEILLANCE SOCIETY.

A CRITICAL CASE STUDY OF THE USAGE OF STUDI VZ, FACEBOOK, AND MYSACE BY STUDENTS IN SALZBURG IN THE CONTEXT OF ELECTRONIC SURVEILLANCE.

ISBN 978-3-200-01428-2

Social Networking Sites and the Surveillance Society.

A Critical Case Study of the Usage of studiVZ, Facebook, and MySpace by Students in Salzburg in the Context of Electronic Surveillance

Christian Fuchs

Salzburg/Vienna, Austria. 2009.
Published by Forschungsgruppe "Unified Theory of Information" - Verein zur
Förderung der Integration der Informationswissenschaften.

ISBN 978-3-200-01428-2

Christian Fuchs. Social Networking Sites and the Surveillance Society. A Critical Case Study of the Usage of studiVZ, Facebook, and MySpace by Students in Salzburg in the Context of Electronic Surveillance.

Published 2009, by Forschungsgruppe Unified Theory of Information (Research Group Unified Theory of Information).

Salzburg and Vienna, Austria. ISBN 978-3-200-01428-2.

This study was conducted at the University of Salzburg, ICT&S Center

Christian Fuchs

University of Salzburg

ICT&S Center

Sigmund Haffner Gasse 18

5020 Salzburg



ICT&S Center

Advanced Studies and Research in Information
and Communication Technologies & Society
University of Salzburg



Creative Commons License. This work is licensed under a Creative Commons Attribution-Noncommercial-No Derivative Works 3.0 Austria License.

<http://creativecommons.org/licenses/by-nc-nd/3.0/at/deed.en>



You are free:

to Share – to copy, distribute and transmit the work

Under the following conditions:

Attribution. You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Noncommercial. You may not use this work for commercial purposes.

No Derivative Works. You may not alter, transform, or build upon this work.

* For any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to this web page.

* Any of the above conditions can be waived if you get permission from the copyright holder.

* Nothing in this license impairs or restricts the author's moral rights.

Christian Fuchs is an Austrian scholar who focuses on media and information society research. He holds a *venia docendi* in ICTs and society-research, is author of many scholarly papers, and of the book "Internet and Society: Social Theory in the Information Age" (New York: Routledge, 2008). He is co-editor of tripleC (Cognition, Communication, Co-operation): Open access online journal for a global sustainable information society (<http://triplec.at>, ISSN: 1726-670X), a transdisciplinary journal that covers research on the challenges that humanity is facing today. It accepts papers from all disciplines and combinations of disciplines carried out with any type of methods that focus on topics relating to contemporary society, contemporary information society, and aspects of communication, media, information, and technology in society.

1. Introduction.....	1
2. Social Networking Sites, Web 2.0, Social Software	4
3. A Critique of Approaches of Research about Integrated Social Networking Sites (ISNS)	11
3.1. Techo-pessimistic Research about Integrated Social Networking Sites.....	11
3.2. Techo-optimistic Research about Integrated Social Networking Sites	16
3.3. Critical Research about Integrated Social Networking Sites	20
4. The Societal Context of Integrated Social Networking Sites (ISNS): Political and Economic Electronic Surveillance.....	22
5. Integrated Social Networking Sites: The Platforms in Our Study.....	34
5.1. studiVZ	34
5.2. Facebook	38
5.3. MySpace	40
5.4. ISNS as Platforms of Economic and Political Surveillance.....	43
6. Integrated Social Networking Sites (ISNS): Research Method.....	45
7. Results	48
7.1. General Characteristics of the Respondents	48
7.2. Surveillance Knowledge	54
7.3. Critique of Surveillance	60
7.4. Usage of studiVZ.....	69
7.5. Usage of Facebook.....	80
7.6. Usage of MySpace	85
7.7. Advantages and Disadvantages of Social Networking Sites	89
7.8. The Usage Rate of Social Networking Platforms in Comparison	97
8. Implications and Conclusions	99
9. Summary	108
9.1. Theoretical Foundations	108
9.2. Research Method	110
9.3. Surveillance Knowledge and Critique of Surveillance.....	110
9.4. studiVZ	111
9.5. Facebook	113
9.6. MySpace	114
9.7. Advantages and Disadvantages.....	115
9.8. Usage in Comparison.....	115
9.9. Implications and Conclusions	115
10. References	118
Annex A: Survey Questionnaire	125

List of Figures

Figure 1. A model of social software and its three subtypes.....	8
Figure 2. Internet advertising profits in the USA (Data Source: IAB Internet Advertising Revenue Report 2007)	33
Figure 3. Gender distribution of the data	48
Figure 4. Status of respondents.....	49
Figure 5. Income of respondents	50
Figure 6. Size of city that respondents have lived in for most of their lifetime	51
Figure 7. Highest educational achievement of respondents' parents.....	52
Figure 8. Occupation of respondents' fathers	52
Figure 9. Occupation of respondents' mothers	53
Figure 10. Usage intensity of integrated social networking platforms.....	53
Figure 11. Intensity of reading the terms of use	54
Figure 12. Knowledge of surveillance #1	55
Figure 13. Knowledge of surveillance #2	56
Figure 14. Knowledge of surveillance #3	56
Figure 15. Surveillance knowledge index (one point for each correct answers to the questions shown in figures 12-14).....	57
Figure 16. Surveillance critique index	63
Figure 17. Share of studiVZ users	70
Figure 18. Knowledge about studiVZ #1	70
Figure 19. Knowledge about studiVZ #2	71
Figure 20. Behaviour concerning the new terms of use of studiVZ	71
Figure 21. Trust in studiVZ	72
Figure 22. studiVZ information behaviour #1	72
Figure 23. studiVZ information behaviour #2	73
Figure 24. studiVZ information behaviour #3	73
Figure 25. studiVZ information behaviour index	74
Figure 26. Usage intensity of Facebook.....	80
Figure 27. Knowledge about Facebook #1	81
Figure 28. Knowledge about Facebook #2	81
Figure 29. Knowledge about Facebook #3	82
Figure 30. Knowledge about Facebook #4	82
Figure 31. Facebook Knowledge Index.....	83
Figure 32. Facebook information behaviour #1	84
Figure 33. Facebook information behaviour #3	84
Figure 34. Usage of MySpace.....	86
Figure 35. MySpace knowledge index.....	86
Figure 36. MySpace information behaviour #1	87
Figure 37. MySpace information behaviour #2.....	88
Figure 38. Major perceived opportunities of social networking sites.....	89
Figure 39. Major perceived risks of social networking sites	93
Figure 40. Comparison of the usage rate of social networking platforms	98
Figure 41. Corporate Watch Organizations: Example 1 (http://www.corpwatch.org)	103
Figure 42. Corporate Watch Organizations: Example 2 (http://www.transnationale.org)	104
Figure 43. Corporate Watch Organizations: Example 3 (http://www.transnationale.org)	104

List of Tables

Table 1. An integrative and dynamic understanding of social software and web 2.0.....	6
Table 2. A typology of Web technologies (Source: Fuchs 2008).....	7
Table 3. Rights guaranteed to corporations by terms of use and privacy policies on studiVZ, Facebook, and MySpace	43
Table 4. Questions on which the surveillance critique index is based	47
Table 5. Representation of different fields of study.....	49
Table 6. Bivariate correlations of surveillance knowledge index and other factors.....	60
Table 7. Critical standpoints towards surveillance #1	61
Table 8. Critical standpoints towards surveillance #2	61
Table 9. Critical standpoints towards surveillance #3	62
Table 10. Critical standpoints towards surveillance #4	62
Table 11. Critical standpoints towards surveillance #5	63
Table 12. Bivariate correlations of surveillance critique index and other factors	67
Table 13. Bivariate correlation between the surveillance knowledge index and the surveillance critique index	68
Table 14. Number of articles on the amendment of the Security Police Act in selected Austrian newspapers (November 22-December 20, 2007; Source: APA DeFacto, search keyword: Sicherheitspolizeigesetz)	69
Table 15. Bivariate correlations about studiVZ	75
Table 16. studiVZ interest groups on the change of the terms of use with most members (accessed on December 7, 2008).....	78
Table 17. Bivariate correlations about Facebook	85
Table 18. Bivariate correlations about MySpace	88
Table 19. Examples for advantages that were listed by the respondents	93
Table 20. Examples for disadvantages that were listed by the respondents.....	96
Table 21. Rights guaranteed to corporations by terms of use and privacy policies on studiVZ, Facebook, and MySpace.....	102

1. Introduction

"Facebook's Roar Becomes a Meow: Putting ads in front of Facebook users is like hanging out at a party and interrupting conversations to hawk merchandise" (Newsweek, October 10, 2008).

"Who Will Rule the New Internet? (...) Still, for wonks like me, it's been riveting to watch three of the most innovative companies in Silicon Valley – each representing a fundamental phase of the information era – battle it out. Apple, Google and Facebook are, respectively, an icon from the pioneering days of personal computers; the biggest, most profitable company yet born on the Web; and a feisty upstart whose name is synonymous with the current migration to social networks. (...) In many ways, these companies are technology's standard-bearers, though their guiding philosophies differ. Google, for instance, advocates an "open" Web and tends to push for open standards and alliances among developers. Facebook, with its gated community of 70 million active users, offers a more controlled experience and, so far at least, wants to keep its users safely within its walls" (Time Magazine, June 4, 2008).

"Facebook: Movement or Business? (...) Yesterday, while he [Facebook's CEO Mark Zuckerberg] talked about the movement and how Facebook's goal was to be a place that promotes sharing and connecting, I couldn't help thinking about Beacon. You might recall that Beacon, an advertising play, was intended to broadcast Facebook users' purchases from external websites. Initially, it was forced on users; there was no opting out. But that turned out to be a nightmare for the young company. Zuckerberg had to apologize and retreat. 'We made a lot of mistakes during the past year,' he admitted yesterday. Clearly, explaining to your users how advertising works on a social network was one of them. (...) Advertising is the essence of Facebook's business; it's the great and shining hope of that company and social media in general. (...) And the only kind of movement that is, is the movement of money" (Time Magazine, July 24, 2008).

"Time's Person of the Year 2006: You. (...) But look at 2006 through a different lens and you'll see another story, one that isn't about conflict or great men. It's a story about community and collaboration on a scale never seen before. It's about the cosmic compendium of knowledge Wikipedia and the million-channel people's network YouTube and the online metropolis MySpace" (Time Magazine, December 13, 2006).

"Facebook, studiVZ, Xing, etc: Study warns: Data are not save enough. Social networks like Xing, studiVZ or Facebook become ever more popular. For maintaining contacts, users reveal private data online – very consciously. Nonetheless more possibilities should be offered for securing and encrypting private details, criticizes the Fraunhofer Institute for Secure Information Technology in a new study" (Bild, September 26, 2009).

"Prostitution on studiVZ? Ever more female students are looking for punters in the community studiVZ in order to finance their studies" (Bild, September 16, 2008).

"The Future President, on Your Friends List. (...) HAVING already launched a generation of Gwen Stefani clones and death-metal bands into fleeting Internet fame, MySpace – the largest social-networking site – is now setting its sights higher: to help elect the next president of the United States. This week, the site will introduce a section dedicated to politics, with an emphasis on the 2008 presidential election. Called the Impact channel, it will be an online version of a town square, a collection of links to political MySpace pages that will make it easier for the site's 60 million American users per month – many of them from the traditionally elusive and apathetic youth demographic – to peruse the personal MySpace pages of, so far, 10 presidential candidates" (New York Times, March 18, 2007).

"Online profile gives China's Premier Wen 'face' with world public. Premier Wen Jiabao has become the sixth most popular politician on the U.S.-based Facebook, a popular social networking site, with more than 44,000 'supporters'" (People's Daily, China, June 3, 2008).

"Love online. (...) My school friend Mayank once swore that he would never date a girl he didn't know well. Imagine my shock when I heard one day, that he is head over heels in love with a girl, whom he met on a social networking site. It all started when he left her a message that praised her profile picture. A few days later, she reverted with a smart answer. Soon they chatted on yahoo, then exchanged cell phone numbers. They chatted into the night and realised that they were in love" (Hindustan Times, India, October 8, 2008).

"Mum no longer knows best as teenage girls turn to online social networking sites for advice. (...) Teenage girls are increasingly turning to social networking websites for guidance on personal matters, rather than seeking advice from their mothers" (Daily Mail, July 22, 2008).

"Nursery nurse has boob job paid by 100 men she doesn't know - thanks to social networking site (...) A mum who had a breast enlargement has 100 men and a social networking site to thank for her new assets" (Daily Mail, July 14, 2008).

“How Obama Really Did It. The social-networking strategy that took an obscure senator to the doors of the White House” (MIT Technology Review, September/October 2008).

“Trouble about user data: The successful student network studiVZ wants to finally earn money – and promptly meets with criticism by data protection specialists” (Die Zeit, December 27, 2007).

Advertising, business, community, privacy concerns, politics, sex, love – these are issues that are associated with the term social networking platforms in popular media clippings, such as the ones just cited. The examples, which certainly have differing depth, character, and quality, show that social networking sites (SNS) and what many term “Web 2.0” have become important topics all over the world and seem to shape economic, political, and cultural communication of contemporary society. Some see SNS as creating new opportunities for democracy, business, or entertainment. Others consider them as risk that will destroy culture and society. Many of these mass-mediated debates are oversimplified and one-sided. But nonetheless they show that there is an interest in the question how online communication tools transform society and our social relations.

Statistics confirm that SNS are very popular.

The Global Top 50 websites, measured by average number of unique pages viewed by user per day and number of unique page visitors (3 month average), include 10 SNS (alexa.com, Global Top 500, accessed on October 20, 2008):

- #5 Facebook (reach: 10.235% of global Internet users, number of unique pages viewed per user per day: 18.4)
- #7 MySpace (6.567%, 31.24)
- #16 Hi5 (2.359%, 34.55)
- #17 QQ (3.061%, 8.19)
- #25 VKontakte (1.3474%, 92.86)
- #28 Orkut Brazil (1.7926%, 39.43)
- #40 Friendster (1.3133%, 25.41)
- #41 Odnoklassniki (1.0918%, 47.65)
- #43 Adult Friendfinder (1.555%, 3.29)
- #45 Orkut India (1.418%, 21.45)

In Austria, there are 7 SNS among the top 50 websites (alexa.com, accessed on October 20, 2008):

- #11 Facebook
- #12 MySpace
- #14 studiVZ
- #17 Netlog
- #22 Szene1
- #40 Adult Friendfinder
- #48 MeinVZ

In Germany, there are 8 SNS among the top 50 websites (alexa.com, accessed on October 20, 2008):

#9 studiVZ
#12 SchülerVZ
#14 MySpace
#15 Wer-kennt-wen
#17 Facebook
#28 MeinVZ
#36 Lokalisten
#44 Odnoklassniki

For Germany, there is another ranking that is based on visits per month (Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern, <http://www.ivw.eu>). For September 2008, there are 9 SNS among the top 50:

#4 studiVZ: 158 583 022 visits
#5 schülerVZ: 134 469 350
#6 Wer-kennt-wen: 112 352 251
#14 MySpace: 49 669 683
#16 meinVZ: 45 558 304
#19 Lokalisten: 30.613.267
#32 StayFriends: 16.730.65
#39 Netlog: 12 663 400
#40 Spin: 12 408 289

In 2007, a survey conducted by the Pew Research Center (N=935) found (Lenhart/Madden 2007):

“55% of [US] online teens use social networks and 55% have created online profiles [in the USA]. (...) 91% of all social networking teens (aged 12-17) say they use the sites to stay in touch with friends they see frequently, while 82% use the sites to stay in touch with friends they rarely see in person. (...) 72% of all social networking teens use the sites to make plans with friends; 49% use the sites to make new friends. (...) 17% of all social networking teens use the sites to flirt. (...) More than three out of four (77%) teens who have created profiles say that their profile is currently visible online, while 21% say their profile is not currently visible. Of those users who have viewable online profiles, more than half (59%) say that their profile is visible only to their friends. Another 40% say that their profile is visible to anyone who happens upon it online. Just 1% of social network users say they do not know who can see their profile“.

Posting messages to a friend’s page or guestbook was the most frequent action (84%), followed by sending private messages (82%), posting to blogs (76%), sending bulletins or posting to groups (61%), poking or giving kudos to someone (33%).

“66% of teens who have created a profile say that their profile is not visible by all Internet users. They limit access to their profiles. 48% of teens visit social networking websites daily or more often; 26% visit once a day, 22% visit several times a day“.

These statistics show that there is a large interest in SNS in the global Internet public, also in the German-speaking world. This interest is also reflected in a rising amount of academic studies of SNS. danah boyd has gathered a collection of research about SNS (<http://www.danah.org/SNSResearch.html>, accessed on October 20, 2008) that lists approximately 150 research papers, 3 books, and 7 research reports published in the years 2003-2008. None of these papers covers the German-speaking world or has German-speaking authors. This shows a lack of research that concerns Austria, Germany, and Switzerland. Therefore the overall motivation for conducting this study is to contribute to research about social networking sites in the German-speaking world.

The specific research questions that are addressed in this study are:

- How does economic and political surveillance frame social networking site usage?
- How knowledgeable are students about surveillance in society?
- How critical are students about the potential surveillance by state and corporation?
- How does the degree of knowledge about surveillance and the degree of critical consciousness on surveillance influence the usage of social networking sites?

SNS are generally focused on young people as target audience. The statistics for the German-speaking world show that studiVZ (studi=students, VZ=Verzeichnis=list, list of students) is a tremendously popular platform. It has been specifically designed as a SNS for students. One of the reasons why this case study is focusing on students is the popularity of SNS among this group. Another reason is that students are traditionally a very critical group in society. 40 years ago, in 1968, student protests reached their climax, especially in France, Germany, and the United States. Topics that were questioned by the protesters included imperialism and the war in Vietnam, a lack of democracy in universities, capitalist consumer culture, standardized Fordist life styles, conservative values, and post-fascists structures. The students' movement and the New Left did not reach the size of a revolutionary movement; nonetheless their activities can be interpreted as anti-capitalist rebellion. Herbert Marcuse (1969: x) argued in this context that "they have taken the idea of revolution out of the continuum of repression and placed it into its authentic dimension: that of liberation". Forty years have passed, capitalist society has changed, neoliberalism has resulted in a large-scale economization and capitalization of society that has also permeated universities and the academic system. Given these circumstances, how important is critical thinking for students today? And how does it influence students' attitudes towards new media such as social networking platforms?

2. Social Networking Sites, Web 2.0, Social Software

Social networking sites are frequently discussed in relation with the categories of Web 2.0 and social software that seem to be a little bit more general than the category of SNS. SNS, just like blogs or wikis, are frequently seen as types of web 2.0 and as social software. However, all of these terms have thus far rather remained vague, which is due to a lack of theoretical foundations (Fuchs 2009).

Some authors tend to argue that the web and software are always social because they incorporate certain meanings and understandings of society (Dourish 2001, Dringenberg 2002, Rost 1997). Their understanding of the social is close to Durkheim's notion of social facts (Fuchs 2009), by which he means

“every way of acting, fixed or not, capable of exerting on the individual an external constraint; or: which is general over the whole of a given society whilst having an existence of its own, independent of its individual manifestation” (Durkheim 1982: 59).

A second group of authors argues that the web and software are only social if they support symbolic interaction (boyd 2005, 2007a; Coates 2005, Webb 2004, Pascu et al. 2007, Shirky 2003). The notion of the social underlying these approaches can be said to be Weberian (Fuchs 2009) because Max Weber argued that not “every type of contact of human beings has a social character; this is rather confined to cases where the actor's behavior is meaningfully oriented to that of others” (Weber 1968: 22-23).

A third group of authors sees social software and web 2.0 as tools that support community-building and online co-operation (Alby 2007, Burg 2003, Fischer 2006, Gillmor 2006, Miller 2005, O’Reilly 2005a, b; Saveri/Rheingold/Vian 2005, Stefanac 2007, Swisher 2007, Kolbitsch/Maurer 2006, Tapscott/Williams 2006). These approaches can be connected on the one hand to Tönnies’ concept of community (Fuchs 2009), by which he understands the “consciousness of belonging together and the affirmation of the condition of mutual dependence” (Tönnies 1988: 69), and on the other hand to Marx’s concept of co-operation (Fuchs 2009):

“By social we understand the co-operation of several individuals, no matter under what conditions, in what manner and to what end. It follows from this that a certain mode of production, or industrial stage, is always combined with a certain mode of co-operation, or social stage, and this mode of co-operation is itself a ‘productive force’” (MEW 3: 50).

These theoretical understandings of the social that underlie definitions of web 2.0 and social software are implicit, a theory of web 2.0 and social software is missing and can be accomplished by dialectically synthesizing the three understandings of the social and applying it to the web (Fuchs 2009, Fuchs, Hofkirchner, Schafranek, Raffl, Sandoval & Bichler 2008).

Actually, it makes sense to develop an integrative view of these three sociality types rather than to look upon them as separate ones. There are two reasons for that: first, the structural, the action, and the cooperation type of sociality can easily be integrated in the way the Aristotelian *genus proximum* and *differentia specifica* are linked together. Durkheim's notion of the *fait social* is the most abstract notion. As such it also applies to actions that – in the sense of Weber – are directed towards other members of society and, beyond that, to the production of common goods within a community in the Tönniesian and Marxian sense.

Defining sociality in the mode Weber does can be seen as making the case for a more concrete and more particular type of sociality than the Durkheimian one: the latter underlies the former. And the Tönnies–Marx concept, finally, is still less general and a subcategory of the Weberian one. Thus they form a kind of hierarchy in which the successor is a logical modification of the predecessor: it takes place under certain constraining conditions.

Second, there is an analogous relationship between the three forms in which information processes occur in society: cognition, communication, and co-operation processes. These processes relate to each other in a way that reflects and resembles the build-up of a complex system. One is the prerequisite for the other in the following way: in order to co-operate you need to communicate and in order to communicate you need to cognise.

Therefore we suggest an integrative view of how sociality is manifested in social software. If the web is defined as a techno-social system that comprises the social processes of cognition, communication and cooperation altogether, then the whole web is Durkheimian, since it is a *fait social*. What in the most widespread usage is called Social Software – that is, that part of the web that realizes communicative as well as cooperative societal roles – is, in addition, social in the Weberian sense, while it is the community-building and collaborative part of the web that is social only in the most concrete sense of Tönnies and Marx too. To put it in another way: that part of the web that deals with cognition only is exclusively Durkheimian without being Weberian, let alone Tönniesian–Marxian; that part that is about communication including cognition is Weberian and Durkheimian; and only the third, co-operative, part has all three meanings. We suggest ascribing to these parts the terms web 1.0, web 2.0 and web 3.0, accordingly (see table 1). Web 1.0 is a computer-based networked system of human cognition, web 2.0 a computer-based networked system of human communication, web 3.0 a computer-based networked system of human co-operation.

*An Integrative
and Dynamic
Approach*

Emile Durkheim: *cognition
as social due to conditioning
external social facts*
Max Weber: *communicative
action*
Ferdinand Tönnies, Karl
Marx: *community-building
and collaborative production
as forms of co-operation*

*The web as dynamic threefold
knowledge system of human
cognition, communication, and
co-operation:*

*Web 1.0 as system of human
cognition.*

*Web 2.0 as system of human
communication.*

*Web 3.0 as system of human co-
operation.*

Table 1. An integrative and dynamic understanding of social software and web 2.0

The level of information (cognition, communication, co-operation) and the type of temporality characterize networked computer technologies. Synchronous temporality means that users are active at the same time (“in real time”), asynchronous temporality that users’ actions are temporally disembedded. In both cases technology enables a spatial disembedding of users. Another aspect of network technologies is the type of relationship they enable: one-to-one-relationships (o2o), one-to-many-relationships (o2m), or many-to-many-relationships (m2m). o2o technologies allow one user to reach single other users, o2m-technologies allow one user to reach many others, and m2m-technologies allow many users to reach many others. The following table provides a typology of Internet technologies characteristic for each of the three aspects of

information. It shows which technologies belong to the three levels of web 1.0, 2.0, and 3.0 (o2o: one-to-one, o2m: one-to-many, m2m: many-to-many).

	Synchronous	Asynchronous
Cognition (Web 1.0)	Peer-to-peer networks for filesharing (o2o, m2o, o2m)	websites (o2m), online journals (o2m, m2m), alternative online publishing (e.g. Indymedia, Altnet, o2m, m2m), online archives (o2m, m2m), e-portfolio (o2m), Internet radio/podcasting (O2m) social bookmarking (o2m, m2m) social citation (o2m, m2m) electronic calendar (o2m) Real Simple Syndication (RSS, o2m)
Communication (Web 2.0)	Chat (o2o, o2m, m2m), instant messaging (o2o, o2m), voice over IP (o2o, o2m, m2m), video conferencing systems (o2o, o2m, m2m)	E-mail (o2o, o2m), mailing-lists (m2m), bulletin board systems (usenet, m2m), web-based discussion boards (m2m), blogs (o2m, m2m), video blogs (v-blogs)/photo blogs (o2m, m2m), group blogs (m2m), social network services (e.g. online dating and friendship services like MySpace, o2o), social guides (o2m, m2m), mobile telecommunication (e.g. SMS and cellular phones; o2o, o2m), online rating, evaluation, and recommendation systems (e.g. tripadvisor, eBay- and Amazon Market Place-user ratings, listing of similar items at Amazon, o2m, m2m)
Co-operation (Web 3.0)	Multi User Dungeons (MUDs) (o2o, o2m, m2m), MUDs Object-Oriented (MOOs) (o2o, o2m, m2m), graphical worlds (o2o, o2m, m2m), MMORPG (Massive Multiplayer Online Roleplaying Games, o2o, o2m, m2m) Synchronous groupware (collaborative real-time editing shared whiteboards, shared application programs, m2m)	wikis (m2m), shared workspace systems (e.g. BSCW) (m2m), asynchronous groupware (m2m), knowledge communities (e.g. Wikipedia)

Table 2. A typology of Web technologies (Source: Fuchs 2008)

Figure 1 shows how the three types of the web are connected in an overall model. In web 1.0, human individuals cognize with the help of data that they obtain from a technologically networked information-space. Web 2.0 as system of communication is based on web-mediated cognition: Humans interact with the help of symbols that are stored, transmitted, and received by making use of computers and computer networks.

Web-mediated cognition enables web-mediated communication and vice versa. There is no communication process without cognition. In web 3.0, a new quality emerges that is produced by communicative actions. Certain cohesion between the involved humans is necessary. Web-mediated communication enables web-mediated co-operation and vice versa. There is no co-operation process without communication and cognition. The three forms of sociality (cognition, communication, co-operation) are encapsulated into each other. Each layer forms the foundation for the next one, which has emergent properties. By the term “web” is not only meant the World Wide Web, but any type of techno-social information network, in which humans are active with the help of networked information technologies.

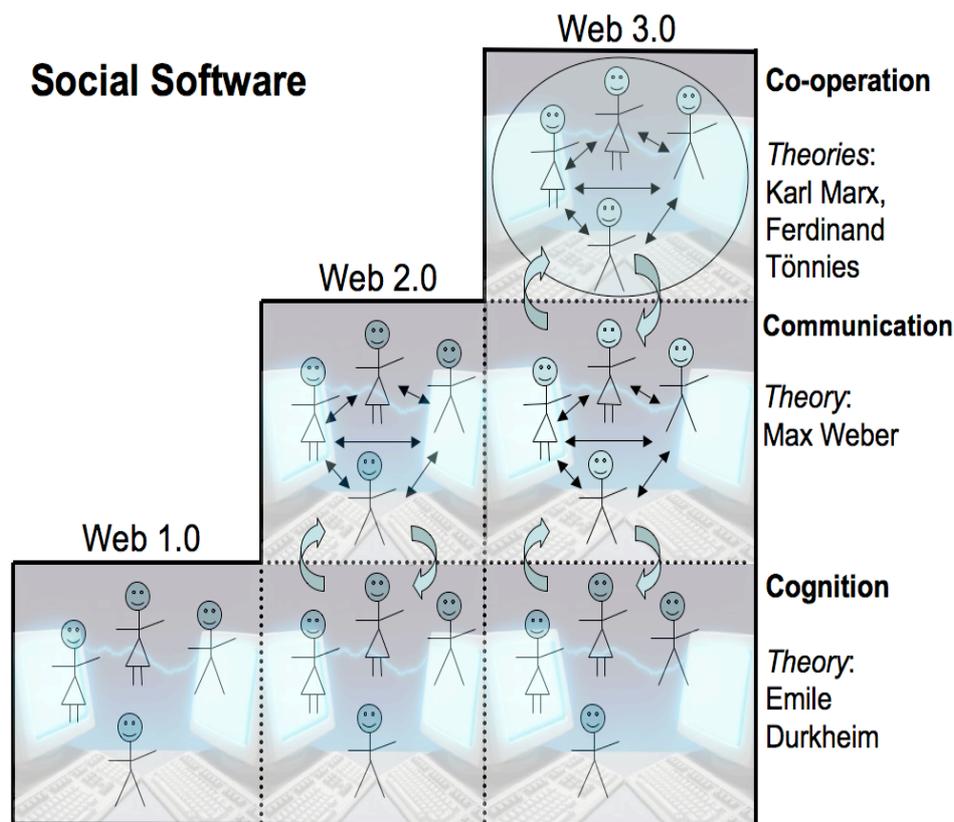


Figure 1. A model of social software and its three subtypes

How does the notion of social networking sites (SNS) fit into this model of the web?

boyd and Ellison (2007) define social network sites as

“web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system”.

boyd’s and Ellison’s definition clearly focuses on platforms such as MySpace, Facebook, Friendster, studiVZ, etc. In network analysis, a network is defined as a system of interconnected nodes (cp. e.g. Wasserman/Faust 1997, Barabási 2003). Therefore, based on a strict theoretical understanding, all networked tools that allow establishing connections between at least two humans, have to be understood as social network

platform. This includes not only the platforms that boyd and Ellison have in mind, but also chats, discussion boards, mailing lists, email, etc – all web 2.0 and 3.0 technologies. Social network site is therefore an imprecise term. Such imprecision can arise from a lack of social theory foundations in SNS research: Definitions are given without giving grounds to them. David Beer (2008b: 519) argues that the definition by boyd and Ellison is too broad and does not distinguish different types of sites such as wikis, folksonomies, mashups, and social networking sites. "My argument here is simply that we should be moving toward more differentiated classifications of the new online cultures not away from them". He suggests to use web 2.0, not SNS, as an umbrella term.

We agree with Beer and therefore consider it feasible to start from a theory of web 1.0, 2.0, 3.0 (Fuchs 2008, 2009, Fuchs, Hofkirchner, Schafranek/Raffl, Sandoval & Bichler 2008). Online platforms such as MySpace or Facebook are web-based platforms of communication and community-building, i.e. not only web 1.0 systems, but also web 2.0 and 3.0 systems. What makes them distinct is that they are integrated platforms that combine many media and information and communication technologies, such as webpage, webmail, digital image, digital video, discussion group, guest book, connection list, or search engine. Many of these technologies are social network-tools themselves. It surely is feasible, as boyd and Ellison argue, that profiles, connection lists, and tools for establishing connections are the central elements, but missing is the insight that platforms such as Facebook are meta-communication technologies, technologies of communication technologies. Tim O'Reilly (2005b) argues in this context that "the network as platform, spanning all connected devices" is a central technological feature of web 2.0.

We find it therefore more appropriate to speak of integrated social networking sites (ISNS). ISNS are web-based platforms that integrate different media, information and communication technologies, that allow at least the generation of profiles that display information that describes the users, the display of connections (connection list), the establishment of connections between users that are displayed on their connection lists, and the communication between users. ISNS are just like all computer technologies web 1.0 systems because they reflect and display dominant collective values of society that become objectified and are confronting users. They are web 2.0 technologies because they are used for communication and establishing connections in the form of connection lists. ISNS are web 3.0 technologies because they allow the establishment of new friendships, communities, and the maintenance of existing friendships. By friendship we mean a continuous social relationship between humans that is based on empathy and sympathy. Therefore ISNS provide means for establishing virtual communities understood as "social aggregations that emerge from the Net when enough people carry on those public discussions long enough, with sufficient human feeling, to form webs of personal relationship in cyberspace" (Rheingold 2000, xx). For Rheingold, a virtual community is not the same as computer-mediated communication (CMC), but continuous CMC that results in feelings of affiliation.

Not all social relations established or maintained on ISNS are forms of community. There might be superficial relations that just exist by a display of connection in the connection list. This can be the case for example if one adds friends of friends whom one has never met and with whom one does not continuously interact, if one adds

people arbitrarily in order to increase the friend's list, or if one adds people who share one's interests, but with whom one also does not communicate. In this case, the usage of ISNS remains on the web 2.0 level. Web 3.0 in the sense of a virtual community is then a mere unrealized potential. It is likely that any concrete ISNS will consist of many loose connections and many virtual communities that exist in parallel. ISNS on the technological level provide potentials for web 2.0 and web 3.0. Only web 2.0 is automatically realized by establishing connections, the emergence of web 3.0 communities on ISNS requires more sustained communicative work so that social bonds emerge. Feelings of community can either emerge on ISNS or can be imported from the outside world. If individuals make use of ISNS for staying in touch with already established friends and contacts more easily and over distance, then existing communities or parts of them are transformed into virtual communities that crystallize on ISNS. If individuals make new social bonds with people whom they did not know in advance and whom they have met on ISNS, then community emerges inherently from ISNS. One can speak of a virtual community in both cases. Web 3.0 is (besides collaborative online labour, which can be found in the case of wikis, but is not a necessary condition) about the production of social bonds and feelings of belonging and togetherness. ISNS support web 3.0, but do not automatically realize web 3.0 communities.

It is clear that all ISNS are inherently used for communication and establishing connections. However, it is not obvious if they are used primarily for maintaining already established contacts, or primarily for establishing new contacts, or for both endeavours. Some speak of social network platforms (for maintaining existing relationships), whereas others of social networking platforms (for building new relationships). However, all networks are based on the permanent reproduction of relations, i.e. on networking, new relations can emerge more or less frequently. Therefore networks and networking cannot be strictly separated and the terminological question can be resolved by arguing that ISNS have potentials for both contact maintenance and formation, i.e. they have a reproductive and a productive role in social relationships. Therefore one aspect of the case study is to clarify what students see as the primary task of ISNS. By asking them what they think is the major advantage of ISNS, we expect to find out how important various types of online contacts are for them.

3. A Critique of Approaches of Research about Integrated Social Networking Sites (ISNS)

The task of this section is to give an overview of existing research about ISNS. It does not discuss all studies that have been undertaken, but categorizes research into three types and gives representative examples for each category:

1. Techno-pessimistic ISNS research
2. Techno-optimistic ISNS research
3. Critical ISNS research

3.1. Techo-pessimistic Research about Integrated Social Networking Sites

This category summarizes approaches that conclude that ISNS are dangerous and pose primarily threats for the users, especially kids, adolescents, and more generally young people. One can also characterize this approach as victimization discourse. Such research concludes that ISNS pose threats that make users potential victims of individual criminals, such as in the case of cyberstalking, sexual harassment, threats by mentally ill persons, data theft, data fraud, etc. Frequently these studies also argue that the problem is a lack of individual responsibility and knowledge so that users put themselves at risk by putting too much private information online and by not making use of privacy mechanisms, for example by making their profile visible for all other users.

Two papers written by Alessandro Acquisti and Ralph Gross represent the ideal type of this kind of research.

Acquisti and Gross conducted an online survey of ISNS users at Carnegie Mellon University (N=294, Acquisti/Gross 2006) and data mining of 7000 ISNS profiles (Gross/Acquisti/Heinz 2005). Privacy policy was considered as a very important issue (average of 5.411 points on a Likert-scale of 7). Users also showed a high concern about the misuse of personal information. The scholars did not find a direct relationship between the intensity of privacy concerns and the likelihood of becoming a Facebook member. Users with higher privacy concerns would be less likely to join ISNS, but not in the case of undergraduates.

“Privacy concerns may drive older and senior college members away from FB. Even high privacy concerns, however, are not driving undergraduate students away from it. Non-members have higher generic privacy concerns than FB members” (Acquisti and Gross 2006: 47). Those users who join the network would not be more likely to exclude personal information from visibility if they have high privacy concerns. “We detected little or no relation between participants’ reported privacy attitudes and their likelihood of providing certain information, even when controlling, separately, for male and female members” (Acquisti and Gross 2006: 50).

The majority of respondents were badly informed about Facebook’s privacy policy and for which purposes their data are used.

“77% of respondents claimed not to have read FB’s privacy policy (the real number is probably higher); and that many of them mistakenly believe that FB does not collect information about them from other sources regardless of their use of the site (67%), that FB does not combine information about them collected from other sources (70%), or that FB does not share personal information with third parties (56%)” (Acquisti and Gross 2006: 53). “Twenty-two percent of our sample do not know what the FB privacy settings are or do not remember if they have ever changed them. Around 25% do not know what the location settings are to summarize, the majority of FB members claim to know about ways to control visibility and searchability of their profiles, but a significant minority of members are unaware of those tools and options. (...)” (Acquisti and Gross 2006: 52).

There would be

“a number of different reasons for the dichotomy between FB members’ stated privacy concerns (high) and actual information hiding strategies (mixed, but often low also for members with high stated concerns). Those reasons include peer pressure and unawareness of the true visibility of their profiles” (Acquisti and Gross 2006: 52).

Females were much less likely to provide their sexual orientation than men. Overall, the authors conclude that there was a lack of privacy concerns of the users.

The data mining analysis provided the following results:

“In general, CMU users of the Facebook provide an astonishing amount of information: 90.8% of profiles contain an image, 87.8% of users reveal their birth date, 39.9% list a phone number (including 28.8% of profiles that contain a cellphone number), and 50.8% list their current residence. The majority of users also disclose their dating preferences (male or female), current relationship status (single, married, or in a relationship), political views (from ‘very liberal’ to ‘very conservative’), and various interests (including music, books, and movies). A large percentage of users (62.9%) that list a relationship status other than single even identify their partner by name and/or link to their Facebook profile” (Gross, Acquisti and Heinz 2005: 75).

78% revealed their full name. 99.94% of the profiles were accessible, also to non-registered users.

The authors give the following potential reasons for the high level of revelation:

“perceived benefit of selectively revealing data to strangers may appear larger than the perceived costs of possible privacy invasions; peer pressure and herding behavior; relaxed attitudes towards (or lack of interest in) personal privacy; incomplete information (about the possible privacy implications of information revelation); faith in the networking service or trust in its members; myopic evaluation of privacy risks; or also the service’s own user interface, that may drive the unchallenged acceptance of permeable default privacy settings” (Gross, Acquisti and Heinz 2005: 73f)

The authors only see individual and interpersonal reasons and attitudes as causes of certain behaviour. They are strictly focusing on individual usage and do not consider that tools and usage are conditioned by the larger societal context, such as corporate profit maximization in the economic systems and state regulation in the political system.

Catherine Dwyer (2007) conducted interviews with SNS users (N=18).

“Although individual concern about the privacy of personal information is very high, participants accepted the tradeoff of access to no-fee sites in exchange for diminished protection of their private information. (...) While most social networking sites did offer privacy options, most participants did not make much of an effort to customize who could view their profile”.

Dwyer, Hiltz and Passerini (2007) conducted a quantitative survey (N=117) of Facebook and MySpace users. They found that Facebook users were more likely to reveal identifying information and MySpace users more likely to reveal relationship status. They report low correlations between privacy concerns and trust into platforms on the one hand and the sharing of profile information with others. An exception was instant messenger screen name, for which there was a high correlation. The conclusion of the paper is that further research is needed.

One problem of the victimization discourse is that it implies young people are stupid, ill informed, that older people are more responsible, that the young should take the values of older people as morally superior and as guidelines, and especially that there are technological fixes to societal problems. It implies that increasing privacy levels technologically will solve the problems and ignores that this might create new problems because this measure might result in less fun for the users, less contacts, and therefore less satisfaction, as well as in the deepening of information inequality. Another problem is that such approaches imply that communication technologies as such have negative effects. These are pessimistic assessments of technology that imply that there are inherent risks in technology. The causality underlying these arguments is one-dimensional: It is assumed that technology as cause has exactly one negative effect on society. But both technology and society are complex, dynamic systems (Fuchs 2008). Such systems are to a certain extent unpredictable and their complexity makes it unlikely that they will have exactly one effect (Fuchs 2008). It is much more likely that there will be multiple, at least two, contradictory effects (Fuchs 2008). The techno-pessimistic victimization discourse is also individualistic and ideological. It focuses on the analysis of individual usage behaviour without seeing and analyzing how this use is conditioned by the societal context of information technologies, such as surveillance, the global war against terror, corporate interests, neoliberalism, and capitalist development.

Such studies are ideological because with their strict focus on the individual user they distract attention from politically important problems and issues. The victimization discourse, just like the yellow press, draws a negative picture of technology and ignores society by focusing just on the individual. That there are some cases of harassment and stalking does not mean that you are at high danger if you reveal certain information and

that therefore all people should always set their profiles to fully private. That there are single examples for such acts or that there is a certain amount of occurrences does not imply that all users are at high risk. People can also be and are also harassed, stalked, etc in non-virtual life. And although there is a certain threat of becoming a victim out on the street, most individuals will not consider never again leaving the house they live in. Just like not leaving your house is not an option, not using the Internet or not using ISNS is not a realistic option for most users. The victimization discourse is morally conservative and as a tendency anti-fun. One needs to change society for finding solutions to problems. There are no technological fixes to societal problems. Societal problems, such as state surveillance after 9/11, corporate interests, or the commodification of personal data in the form of spam and advertising, that frame Internet use are political problems, not individual ones.

Jones, Millermaier, Goya-Martinez and Schuler (2008) conducted a content analysis of MySpace sites (N=1378).

“The overwhelming majority of profiles sampled (98.3 percent) were public and nearly two-thirds (61.5 percent) appeared to display a self-portrait as the user’s identifying image. An additional 14.4 percent included an image of the user with a friend or romantic partner. (...) most were more conservative in their disclosure of more sensitive identifying information. On their profile pages, 78.4 percent of users in the sample displayed their first name while only 11.0 percent disclosed their full name. Approximately two-thirds of users sampled (64.5 percent) displayed their first name as their online user name specifically, while a mere 1.9 percent of users used their full name as their user name. Less than one percent (0.80 percent) used a realistic name, although 3.60 percent of user names were a combination of a nickname with a real name. About 14.6 percent used an online handle (an ID name used on Internet sites) as their user name, while 9.4 percent used a phrase (...) It is interesting to note that only 2.7 percent outright displayed their IM name given the apparent preference for this method of communication. An even smaller proportion of users, only one percent, included an e-mail address in their profile. MySpace provides a space in the profile to list a URL that profile viewers may wish to visit. (...) The inclusion of offline contact information was an anomaly in user profiles. Only three users displayed their telephone number. (...) Users boasted a large number of friends in their profiles with an average of 145 per person. (...) Consistent with Stutzman’s (2006) findings on self-disclosure, MySpace users showed high disclosure of personal information in categories such as race, sexual orientation, body type, height, relationship status, personal photo and first name. (...) Nevertheless, this study did not find any evidence of widespread disclosure of information that would be easily used for stalking or other forms of offline harassment”.

Alice Marwick (2008) argues that politics and the media have created a moral panic about online predators that want to sexually abuse kids with the help of MySpace. Ybarra and Mitchell (2008) conducted a survey (N=1588) that showed that 4% of users reported an unwanted sexual solicitation on an ISNS and 9% an online harassment on an ISNS. The authors conclude that broad claims of victimization risk are not justified and that focusing on solving psycho-sociological problems of youths instead of blaming the Internet is appropriate. Rosen (2006) found that seven to nine percent of teens have

been approached sexually on MySpace. Therefore Marwick concludes:

“Thus, I conclude that the furor over MySpace is disproportionate to the amount of harm produced by the site. Indeed, the furor over online predators seems also to be disproportionate. Rather than focusing on nebulous ‘predators,’ it seems that parents, teachers, and social workers should emphasize identifying and preventing abuse in specific, local community settings. (...) while online predators do not represent an epidemic or socially significant problem, child pornography and child abuse are important social issues that require attention. However, they are not caused by minors using MySpace, and preventing children from using social networking sites will do nothing to end these problems. (...) Prohibiting teens from using MySpace will not prevent them from using the site, and instead will dissuade them from talking about any problems that occur”.

These studies show that ISNS are not a real threat for teenagers and others, and that the victimization discourse is a construction that serves ideological purposes, i.e. the distraction from more serious issues such as corporate interests and state surveillance, is a projection of the fears and problems of adults and of their desire to control the young, and a moral Puritanism that is anti-fun and anti-sex. Ideology in this respect means that there is a difference between claims (ISNS as threat) and actuality (actual degree of abuse, threats, etc).

Further examples for the techno-pessimistic victimization discourse on ISNS can be given. This is not a complete discussion. It is only exemplary. They generally tend to stress that students put themselves at risks of stalking, sexual abuse, etc and have low privacy concerns and therefore make their profiles visible to the public.

Frederic Stutzman (2006) conducted a survey (N=200) of students who use Facebook. He found that a “large number of students share particularly personal information online” such as relationship status, location information, and political views. Nonetheless there would be a strong agreement to the statement that it is important to protect identity information (4.21 of 5 points, 5=strongly agree).

Tufekci (2008a) (N=704) reports results from a quantitative survey. 94.9% of the responding Facebook users used their real names. 21.3% indicated their phone number, 12.5% their address, 46.3% their political view, 72.2% their sexual orientation, 75.6% their romantic status.

“We also found that the perceived likelihood that future employers, government, corporations, or romantic partners would see their profile did not have an impact on the visibility of their profiles. The students also did not find any of those scenarios very likely, except for future romantic partners. (...) As in previous research, we found that general privacy concerns were not of much relevance to students’ decisions regarding disclosure” (Tufekci 2008a: 31ff).

Tufekci (2008b) conducted qualitative focus group interviews with 51 SNS users and a quantitative survey (N=713). “The most significant predictor of SNS use in the logistic models, besides gender, was the tendency to use the Internet for expressive purposes: reading blogs, creating web pages, emailing, etc.” (Tufekci 2008b: 560). The author

also found that “higher online privacy concerns somewhat lowered the odds that a student would use SNS” (Tufekci 2008b: 556).

Such research is also contradicted by other studies: Hinduja and Patchin (2008) conducted a content analysis of MySpace profiles (N=9282).

“In addition, this research endeavor also revealed that almost 40% of youth set their profile to private, thereby limiting access to their information to those approved as friends. Of those that were not set to private and therefore viewable by anyone, over 81% of adolescent users included their current city while 28% also listed their school. Less than 9% of youth included their full name (38% listed their first name) and approximately 57% included a photograph of themselves (including over 5% wearing a swimsuit or underwear). Very few youth included ways to contact them outside of MySpace: 4% included an instant messaging screen name, 1% included an email address, and less than one-third of 1% included a phone number. Finally, a number of youth revealed on their profiles that they had used various illicit substances (18% used alcohol, 8% used tobacco, and less than 2% used marijuana)” (Hinduja/Patchin 2008: 140).

The authors conclude that “the vast majority of youth seem to be responsibly using the web site” (Hinduja/Patchin 2008: 140).

3.2. Techno-optimistic Research about Integrated Social Networking Sites

This second approach questions the first one and argues that the victimization discourse aims at the control of teenagers and young people by older persons and that the latter construct the Internet as dangerous in order to be able to exert control, take a moral conservative and puritan position, and to prohibit or limit fun and online excitement. The implication is that ISNS should be autonomous spaces that empower young people and help them to construct their own autonomy that they need in order to become adults and to strengthen their personality. The techno-optimistic discourse is one of empowerment. It stresses the potential of technology for autonomy, personal development, freedom; the formation, maintenance, and deepening of communities, love, or friendships. This discourse assesses ISNS fairly positive, it mainly sees advantages, and considers disadvantages as ideological constructs or as minor issues.

The works of danah boyd represent the ideal type of this kind of research. Donath and boyd (2004) hypothesize that social networking platforms are technologies that are more suited for forming and maintaining weak ties than strong ties. boyd (2008b) argues that teenagers are controlled in school by teachers and at home by parents and therefore seek autonomous spaces that they need for identity formation and their personal development. This would be one of the main reasons for the popularity of SNS.

“What is unique about the Internet is that it allows teens to participate in unregulated publics while located in adult-regulated physical spaces such as homes and schools. Of course, this is precisely what makes it controversial. Parents are seeking to regulate teens behavior in this new space; and this, in turn, is motivating teens to hide” (boyd 2008b).

It would be rather harmful if parents try to control these spaces:

“Many adults believe that these restrictions are necessary to prevent problematic behaviors or to protect children from the risks of society. Whether or not that view is valid, restrictions on access to public life make it difficult for young people to be socialized into society at large. (...) We are doing our youth a disservice if we believe that we can protect them from the world by limiting their access to public life. They must enter that arena, make mistakes, and learn from them. Our role as adults is not to be their policemen, but to be their guide“ (boyd 2008b).

boyd (2007b) formulates the hypothesis that MySpace users are primarily kids with working class background. MySpace users would also include music freaks and “kids who are socially ostracized at school because they are geeks, freaks, or queers”. She calls these teens the subaltern teens. Hegemonic teens would mainly use Facebook.

“These kids tend to come from families who emphasize education and going to college. They are part of what we'd call hegemonic society. They are primarily white, but not exclusively. They are in honors classes, looking forward to the prom, and live in a world dictated by after school activities”.

Hegemonic kids on Facebook would have a negative view of the subaltern kids on MySpace. boyd (2004) characterizes Friendster as a site for self-presentation, a site for connection, and a site with faked profiles (Fakester). boyd (2006a) found in a case study of Friendster that the most common reasons for adding someone to friends lists were that these people were actual friends, acquaintances, family members, or colleagues. Social networking platforms like MySpace would be “full-time always-on intimate communities” (boyd 2006b). boyd and Heer (2006), based on participant observation including interviews, survey, and focus groups of 200 Friendster early adopters, argue that the Fakester profiles served playful purposes and were viewed by their creators as artistic creations.

David Beer (2008b) argues that the research agenda outlined by boyd and Ellison (2007) is too much focused on the user and excludes macro-contexts.

“By focusing solely upon the user, which is what boyd and Ellison's closing section on 'future research' suggests, we are overlooking the software and concrete infrastructures, the capitalist organisations, the marketing and advertising rhetoric, the construction of these phenomena in various rhetorical agendas, the role of designers, metadata and algorithms, the role, access and conduct of third parties using SNS, amongst many other things. (...) Capitalism is there, present, particularly in the history, but it is at risk of looming as a black box in understandings of SNS. (...) This is what is missing, a more political agenda that is more open to the workings of capitalism. At the moment we are informed largely by accounts of these spaces where we can connect, spaces that are host to new or remediated social connections, spaces that are democratic and mutually owned – the direction boyd and Ellison intimate and their focus solely upon the user looks to perpetuate this agenda even if unintentionally, at least, in my reading, that is the risk. My feeling is that the dominant visions of the democratization of the web

toward a model of 'collaborative' or 'collective intelligence' needs to be questioned with some rigour" (Beer 2008b: 523-526).

In short, Beer's critique of boyd and Ellison is that the approach is individualistic, too optimistic, and ignoring that ISNS are embedded into capitalism and are primarily corporations with capitalist interests.

Just like techno-pessimism, techno-optimism is a one-sided discourse that ignores the multiple, contradictory causality of complex systems (Fuchs 2008). Just like that it is unlikely that ISNS only put users at risk, it is one-dimensional to assume and unlikely that ISNS only empower users. The empowerment discourse is also individualistic because it focuses research primarily on how individuals use ISNS for making connections, maintaining or recovering friendships, falling in love, creating autonomous spaces, etc. It does not focus on how technology and technology use are framed by political issues and issues that concern the development of society, such as capitalist crises, profit interests, global war, the globalization of capitalism, or the rise of a surveillance society (cp. Fuchs 2008).

Further examples for the techno-optimistic empowerment discourse on ISNS can be given. Such studies stress especially the opportunities for forming and maintaining social relationships of various kinds. The following discussion is not complete, i.e. only exemplary, and is presented chronologically.

Donath and boyd (2004) hypothesize that social networking platforms are technologies that are more suited for forming and maintaining weak ties than strong ties. Ellison, Steinfield, and Lampe (2007) conducted empirical research on the quality of social connections in the social networking platform Facebook. Their method was a quantitative empirical online survey with a random sample of 800 Michigan State University undergraduate students, from which 286 completed the survey. The major result of the study was that "participants overwhelmingly used Facebook to keep in touch with old friends and to maintain or intensify relationships characterized by some form of offline connection such as dormitory proximity or a shared class". There was a stress on "connecting with offline contacts as opposed to meeting new people". Facebook users used the platform for maintaining strong social ties and forming weak social ties. Facebook

"may help individuals to maintain pre-existing close relationships, just as it can be used as a low-maintenance way to keep tabs on distant acquaintances. (...) Online interactions do not necessarily remove people from their offline world but may indeed be used to support relationships and keep people in contact, even when life changes move them away from each other" (Ellison/Steinfield/Lampe 2007).

Another survey (N=1440, Lampe, Ellison and Steinfield 2006a) at Michigan State University showed that students have high confidence that their profiles describe them accurately (mean=4.16 of 5). There was high agreement to the statement that one engages in keeping in touch with old friends and checking out the Facebook profiles of people one has met in person.

“Given these indicators, we find support for the idea that Facebook members are using the site to engage in social searches, i.e. find out more about people in their offline communities. Social browsing, finding people online for offline encounters, was widely reported as an unlikely use by the survey respondents” (Lampe/Ellison/Steinfeld 2006a: 170).

Lampe, Ellison and Steinfeld (2006b) analyzed 30773 Facebook profiles. They found that

“there is an association between how many items a person lists in their open-ended profile fields and the number of friendship links they have. (...) We found that populating profile fields on Facebook is positively related to the number of friends a user will have listed. The amount of information posted in open-ended fields does not affect the number of friends when added to the indices of the presence of information in the profile fields” (Lampe/Ellison/Steinfeld 2006b: 441).

Referent information (hometown, high school, residence, field of study) had the greatest positive influence on the number of friends, followed by contact information (relationship status, type of contacts one looks for, website, address, birthday, AIM, email), and interests (interests, music, books, TV shows, movies, political views, favourite quotes, about me).

Valkenburg, Jochen and Alexander (2006) have conducted a psychological survey of ISNS users (N=881) and found that positive feedback on profiles enhances adolescents’ self-esteem and wellbeing, whereas negative feedback decreases self-esteem and wellbeing.

Di Gennaro and Dutton (2007) present data from the Oxford Internet Survey that shows that in 2005, 20 percent of British Internet users, which are 12 percent of all Britons, have met new people online. They predict that the rise of social networking sites will further advance this rate.

Humphreys (2007) used participant observation, user observations, and in-depth interviews, for studying the use of the mobile SNS Dodgeball (N=21). He found that Dodgeball enabled users to “coordinate face-to-face meetings among groups of friends” and that third spaces (certain bars, cafés) emerged that “allow for habitual, dynamic, and technologically-enabled face-to-face interaction among loosely tied groups of friends”.

“Dodgeball is not contributing to the further atomization of mobile phone users in public spaces, but it is not necessarily contributing to their collectivization, either. Instead, Dodgeball is primarily connecting Dodgeball users to one another and not to the general urban public, thus leading to a kind of social molecularization. As an MSNS, Dodgeball becomes another means of maintaining and reinforcing social bonds. Even when my informants did meet new people through Dodgeball, these people were fairly demographically similar. While urban areas are diverse environments, Dodgeball may contribute to an illusion of ‘looser’ sociality despite reinforcing homophilous tendencies” (Humphreys 2007).

Sonia Livingstone (2008) conducted qualitative interviews with ISNS users (N=16, age between 13 and 16) and found out that younger teenagers prefer identity management and aesthetic concerns on their profiles, whereas older teenagers find their personal links more important. Teenagers would not be unconcerned about their privacy on ISNS. "The point is that teenagers must and do disclose personal information in order to sustain intimacy, but they wish to be in control of how they manage this disclosure" (Livingstone 2008: 405). They typically want to have their profile public for friends and private to persons. They, according to Livingstone, distinguish between different degrees of closeness to their friends on SNS and find it frustrating that most ISNS do not allow discriminating levels of access to personal information within the list of friends.

"Unsurprisingly, then, when asked whether they would like to change anything about social networking, the operation of privacy settings and provision of private messaging on the sites are teenagers' top priorities, along with elimination of spam and chain messages – both intrusions of their privacy" (Livingstone 2008: 406).

Raacke and Bonds-Raacke (2008) conducted a study that showed that the majority of college students use ISNS for making new friends, locating old friends, and staying in touch with existing friends.

Thelwall (2008) in two waves analyzed 15043 and 7627 MySpace profiles. He found that the median number of friends of people who have at least two friends is 27 and that the median age is 21.

Zhao, Grasmuck and Martin (2008) analyzed 63 Facebook profiles and conclude that identity is shown and not told by stressing group belonging and personal identities over personal narratives.

3.3. Critical Research about Integrated Social Networking Sites

Based on a synthesis of definitions (Gandy 1982: 2, Hardt 1992: x, Kellner 1995: 4, Kellner/Durham 2006: xiv, Knoche 2005: 105, Winter 2004: 118-120), critical media and communication theory and research can be defined as studies that focus ontologically on the analysis of media, communication, and culture in the context of domination, asymmetrical power relations, exploitation, oppression, and control by employing epistemologically all theoretical and/or empirical means necessary in order to contribute at the praxeological level to the establishment of a participatory, co-operative society. This definition is fairly broad and allows to combine different concepts that come from different critical backgrounds, such as for example – to name just some of many – audience commodity, media accumulation strategies, commodity aesthetics, culture industry, true and false consciousness/needs, instrumental reason, technological rationality, manipulation, ideology critique, dialectical theatre, critical pedagogy, aura, proletarian counter-public sphere, multiple publics, emancipatory media usage, repressive media usage, alternative media, radical media, fetish of communication, ideological state apparatuses, the multitude, the circulation of struggles, hegemony, structure of feelings, articulation, dominant reading, oppositional reading, negotiated reading, capital-accumulation function of the media, commodity

circulation function of the media, legitimatizing function of the media, advertising- and public-relations function of the media, regenerative function of the media, propaganda model of the media, communicative action, dialogic communication, discursive communication, communication empire, transnational informational capitalism, working class culture, subculture, etc, under one united umbrella definition that sees them as differentiated unity in plurality that is termed critical communication and media studies.

Critical studies have to do with the Marxian

“categoric imperative to overthrow all relations in which man is a debased, enslaved, abandoned, despicable essence, relations which cannot be better described than by the cry of a Frenchman when it was planned to introduce a tax on dogs: Poor dogs! They want to treat you as human beings!” (MEW 1: 385¹).

If we understand Marxian critique based on the critical categoric imperative as the critique of all forms of domination and all dominative relationships, then all critical theory/research and therefore also all critical media and communication studies are Marxian-inspired.

One important aspect of critical studies is that they focus on the critique of society as totality, i.e. they frame research issues by the macro context of the development dynamics of society as a whole. Herbert Marcuse has argued in this respect that critical research analyzes and criticizes “the totality of the established world” (Marcuse 1937/1988: 134). “It is more due to the theory’s claim to explain the totality of man and his world in terms of his social being” (Marcuse 1937/1988: 134f). This focus of critical research implies that the dominant two types of ISNS research, as conducted by techno-pessimists like Alessandro Acquisti and Ralph Gross and techno-optimists like danah boyd, is uncritical because it does not focus on how ISNS are conditioned by the totality of society. Counter to these uncritical approaches, it is the intention of this study to make a critical analysis, which means to analyze how repressive qualities of the totality, especially state surveillance after 9/11, capital accumulation and corporate profits, and economic surveillance, shape ISNS. ISNS usage is conditioned by the capitalist economy, the political system, and dominant cultural value patterns and conflicts.

The foundation of critical ISNS research, which some might find discomfoting, is that there are no easy solutions to societal problems. Such problems will neither disappear by using more or less technology or using technology differently nor by changing individual behaviour. More fundamental political changes are necessary. The implication is that as long as there are corporate interests in technology and as long as there is what some now term a new imperialism (Harvey 2003, Panitch/Leys 2004, Wood 2003) that has created the conditions for 9/11, the wars in Iraq, Afghanistan and that creates a vicious mutual reinforcing cycle of terror and war, ISNS users will be confronted by economic and political surveillance. As long as states see increasing surveillance as an increase of security, there will be a decrease of privacy and freedom.

¹Translation from: <http://www.marxists.org/archive/marx/works/1843/critique-hpr/intro.htm>, accessed on September 30, 2008.

As long as ISNS are objects of capital accumulation, users will witness how their data are collected, analyzed, statistically evaluated, and sold as commodities. Commercial ISNS are profit-oriented and therefore aim at gathering as much personal data as possible in order to sell it to third parties that advertise on the platform so that profit can be generated. The real threat is that ISNS users become objects of state surveillance because providers pass on their data to the police or the secret service and objects of economic surveillance that drives capital accumulation. Given the current societal framework, these processes are almost inevitable. The real threats are corporate interests and state surveillance. The problem is not the individual behaviour of young people. If we want to protect them, then we need to change society. The crucial point here is that no matter if users set their profiles to visible or invisible, commercial ISNS will always pass on the data to the state as long as there are interests in establishing a "surveillance society", and to other companies and advertisers, as long as they have a profit interest. Therefore the only solution to privacy threats is to overcome new imperialism, surveillance society, and capitalism. If research just focuses on issues such as individual privacy settings and how they can be adjusted, or individual empowerment, then one neglects these issues and therefore conducts uncritical research.

Critical research sees the relationship of society and technology as dialectical, i.e. as a process of mutual shaping (Fuchs 2008). Technological determinism is "the idea that technology develops as the sole result of an internally dynamic, and then, unmediated by any other influence, molds society to fit its pattern" (Winner 1980/1999: 29). Both techno-optimism and techno-pessimism are forms of technological determinism. In contrast, dialectical analyses of technology and society constitute a form of realism, they identify contradicting forces and potentials and show how these contradictions exactly take form, and to which extent each dialectical pole is developed (Fuchs 2008).

4. The Societal Context of Integrated Social Networking Sites (ISNS): Political and Economic Electronic Surveillance

Surveillance means that someone "is seen, but he does not see; he is the object of information, never a subject in communication" (Foucault 1977: 200). Surveillance is a power that is "capable of making all visible, as long as it [...] [can] itself remain invisible" (Foucault 1977: 214). Foucault considers contemporary society as society of surveillance and as disciplinary society. He makes clear that surveillance is a repressive, coercive process:

"Our society is one not of spectacle, but of surveillance. (...) the individual is carefully fabricated in it, according to a whole technique of forces and bodies" (Foucault 1977: 217).

For Giddens, surveillance means the accumulation of information defined as symbolic materials that can be stored by an agency or collectivity as well as the supervision of the activities of subordinates by their superiors within any collectivity (Giddens 1981: 169). The modern nation state would from its beginning have been an information society because it would collect and store information on citizens (births, marriages, deaths, demographic and fiscal statistics, 'moral statistics' relating to suicide, divorce, delinquency, etc.) in order to organize administration.

“Surveillance as the mobilising of administrative power – through the storage and control of information – is the primary means of the concentration of authoritative resources involved in the formation of the nation-state” (Giddens 1985: 181).

Other than Foucault, Giddens does not see surveillance as something entirely negative and dangerous and argues that surveillance phenomena also enable modern organization and simplify human existence. Giddens and others do not use surveillance as a critical, but a relatively neutral notion. The violent and coercive aspects of surveillance cannot be criticized adequately within such frameworks. To limit the notion of information society to surveillance is a narrow perspective that ignores the specific role of knowledge and information technologies in contemporary capitalism.

For Kevin Haggerty (2006), the employment of the category of Bentham’s panopticon introduced by Foucault into surveillance studies is not suitable for analyzing surveillance in the information society because surveillance would no longer serve the single coherent purpose of control as with e.g. weblogs and webcams more and more people are viewers at home, work, or leisure (cf. also Bogard 2006 who argues with Deleuze and Guattari that surveillance today is not only repressive capture, but also a line of flight from oppression; Koskela 2006). For characterizing the plural character of surveillance, Haggerty and Ericson (2000) have coined the concept of the surveillance assemblage. Haggerty (2006) argues that private actors now also conduct surveillance. His notion of surveillance is close to the one of Giddens.

The notion of surveillance as potentially empowering has also been taken up in ISNS research: Anders Albrechtslund (2008) argues that social networking sites show that surveillance is not necessarily disempowering, but is “something potentially empowering, subjectivity building and even playful”.

“Online social networking can also be empowering for the user, as the monitoring and registration facilitates new ways of constructing identity, meeting friends and colleagues as well as socializing with strangers. This changes the role of the user from passive to active, since surveillance in this context offers opportunities to take action, seek information and communicate. Online social networking therefore illustrates that surveillance – as a mutual, empowering and subjectivity building practice – is fundamentally social” (Albrechtslund 2008).

Albrechtslund speaks in this context of participatory surveillance:

“The practice of online social networking can be seen as empowering, as it is a way to voluntarily engage with other people and construct identities, and it can thus be described as participatory. It is important to not automatically assume that the personal information and communication, which online social networking is based on, is only a commodity for trading. Implicit in this interpretation is that to be under surveillance is undesirable. However, to participate in online social networking is also about the act of sharing yourself – or your constructed identity – with others. (...) In this case, participatory surveillance is a way of maintaining friendships by checking up on information other people share” (Albrechtslund 2008).

One can either define surveillance as a neutral term or as a term that signifies a coercive process that always is embedded into dominative systems. The first definition, as chosen by e.g. Giddens, Haggerty, or Albrechtslund, poses the danger that developments such as limitations of basic freedoms by state or corporate surveillance are put on the same level with information gathering strategies that do not coerce people or threaten their privacy and freedoms so that developments into the first direction can no longer be adequately criticized. Therefore we have chosen to define surveillance as a critical concept that allows us to question coercive forms of information gathering.

Electronic surveillance by nation states and corporations aims at controlling the behaviour of individuals and groups, i.e. they should be forced to behave or not behave in certain ways because they know that their appearance, movements, location, or ideas are or could be watched by electronic systems. In the case of political electronic surveillance, individuals are threatened by the potential exercise of organized violence (of the law) if they behave in certain ways that are undesired, but watched by political actors (such as secret services or the police). In the case of economic electronic surveillance, individuals are threatened by the violence of capital and the market that wants to force them to buy or produce certain commodities and help reproduce capitalist relations by gathering and using information on their economic behaviour with the help of electronic systems. In such forms of surveillance violence and heteronomy are the *ultimo ratio*, whereas in private forms of displaying oneself on the Internet violence in most cases does not play an important role. In the second case the individuals being watched agree to it and control surveillance technologies themselves, in the first case they do not and in most cases they do not even know that they are under surveillance. Hence I would distinguish between electronic monitoring as a general notion of providing and gathering information with the help of electronic systems and electronic surveillance as the gathering of information on individuals or groups in order to control their behaviour by threatening the exercise of institutionalized violence or exercising economic violence. We agree with Ogura (2006) that a common characteristic of surveillance is the management of population based on capitalism and/or the nation state.

David Lyon (2003, 5; cf. also 2001, 2, 16) defines surveillance as “routine ways in which focused attention is paid to personal details by organizations that want to influence, manage, or control certain persons or population groups”. Although Lyon does not speak of surveillance as form of violence, coercion is an immanent aspect of his notion of surveillance. Surveillance means the collection of data on individuals or groups that are used to control and discipline behaviour by the threat of being targeted by violence. Surveillance operates with uncertainty, invisibility, and psychological threats. Foucault (1977) has stressed that discipline and potential punishment are important aspects of surveillance in the sense that the latter aims at the control and subjugation of bodily movements. One can add that besides behaviour also mental activity and communication shall be controlled by surveillance.

Surveillance is an expression of instrumental reason and competition because it is based on the idea that others are watched and data on their behaviour, ideas, look, etc. are gathered so that they can be controlled and disciplined and choose certain actions

and avoid others that are considered as undesirable. Competitive interests and behaviours are involved, the controlling group, class or individuals try to force the surveilled to avoid certain actions by conveying to the latter that information on them is available that could be used for actions that could have negative influences on their lives. Surveillance operates with threats and fear. It is a form of psychological and structural violence that can turn into physical violence.

David Lyon (1994, 2001) has argued that the intensification of surveillance by computer technologies has resulted in a surveillance society. Surveillance is not the only main feature of contemporary society, there are a whole lot of others such as capital, knowledge, networks, flows, globalization, neoliberalism, etc. Hence the notion grasps just one feature, which is nonetheless a quite important and dangerous one.

After September 11, 2001, electronic surveillance has been intensified (Cf. Ball and Webster 2003, Lyon 2003, Webb 2007). Here are some examples:

- In Newham, London, UK CCTV cameras are linked to the Mandrake facial recognition software (Gray (2003) speaks of the rise of a facial recognition society in which thoughts that normally remain hidden to others are made visible with the help of new technologies). The UK has been at the forefront in the installation of CCTV (Gras 2004, Webster 2004).
- Biometrical iris scanners or facial recognition software for identity matching have been installed in numerous airports such as Frankfurt, Gatwick, Heathrow, Amsterdam Schiphol, Sydney, Melbourne, Boston Logan, or Manchester.
- In Europe, the USA, and Canada, biometric passports with digital photos and RFID computer chips that store personal data have been introduced. In Canada, such passports have no chip. Biometric passports shall make passports fraud resistant and enable identity authentication.
- Immediately after 9/11, many Internet Service Providers agreed to install Carnivore computers, a data surveillance system operated by the FBI.
- Based on the Alien Registration Act, fingerprints of several ten thousand Arab immigrants were taken after 9/11 in the USA.
- Section 201 of the USA Patriot Act that was passed in October 2001 allowed the interception of wire, oral, and electronic communications relating to terrorism if approved by a federal judge.
- Section 210 widened the scope of subpoenas for records of electronic communications to include e.g. identifying numbers such as temporary IP addresses
- Section 217 allowed the interception of communications of a person who trespasses (access without authorization) a financial or US government computer.
- Section 503 allowed the US state to collect DNA samples from offenders of terrorism and violent crime.
- Section 505 of the Patriot Act that allowed the FBI to obtain data on any user from Internet Service Providers was declared unconstitutional in 2004.
- Section 814 set the punishment for attempting to damage protected computers to up to 10 years in prison and the punishment for unauthorized access and subsequent damage to up to 5 years in prison.
- In late 2005 and in 2006, there were press reports and concerns that the NSA performed warrantless eavesdropping on citizens' phone calls and Internet traffic (cf.

e.g. "Bush Lets US Spy on Callers Without Courts", *New York Times*, December 16, 2005).

- The US-VISIT program requires travellers from certain countries entering the USA to have their fingers digitally scanned and to be digitally photographed.
- In 2002, the Bush administration planned to implement the Terrorism Information and Prevention System in which data on suspicious citizens gathered by workers who had access to private homes (such as mailmen) would have been stored in databases.
- Total Information Awareness (TIA) was a project started after 9/11 by the US Information Awareness Office that aimed at identifying potential terrorists by methods of collecting information and combining and assessing data from different already existing databases. Following heavy public criticism and civil rights concerns, Congress suspended the program in spring 2003.
- In 2004, an agreement between the USA and the EU was signed that required European airlines to transmit Passenger Name Records (PNRs) on transnational flights to the US in advance of flights to US authorities. PNRs include 34 data sets such as full name, passport details, date and place of birth, contact details, address, phone number, e-mail address, flight data, form of payment. In 2006, the European Court of Justice annulled the agreement and a new temporary agreement was reached in fall 2006. The main difference to the old agreement is that data is passed from airlines to the US Department of Homeland Security (DHS) based on requests (data push), whereas in former times the latter had continuous access to the databases of the first (pull). The requests are not limited in number, rather transfer is defined as required by DHS.
- In spring 2006, the EU adopted the Data Retention Directive that requires all member states to pass bills that require communication providers to store connection data (identity of source and receiver of a communication, date, time, length, provider, location data of mobile phones during calls, etc.) of all phone and internet communications for a period between 6 months and 2 years.
- The Computer Assisted Passenger Prescreening System (CAPPS) has been introduced in US aviation. It compares PNRs with data of the FBI and other agencies in order to calculate a terrorism risk score so that extra-screening of certain people and their luggage becomes possible.
- The Echelon system is a UK-US spy network that can intercept radio and satellite communication, phone calls, e-mails, and Internet data (cf. Lyon 2003, 96f; Wright 2005). Not much is known about this system, its functions and hence one can only speculate on its increasing importance after 9/11.

As already mentioned, the European Commission passed the Data Retention Directive (2006/24/EC) on March 15, 2006, which requires all member states to pass laws that guarantee that information and communication service providers store source, destination, and other data on a communication for at least 6 months. The data that needs to be stored includes:

- “(a) data necessary to trace and identify the source of a communication (...)
- (b) data necessary to identify the destination of a communication (...)
- (c) data necessary to identify the date, time and duration of a communication (...)
- (d) data necessary to identify the type of communication (...)
- (e) data necessary to identify users’ communication equipment or what purports to

be their equipment

(f) data necessary to identify the location of mobile communication equipment².

“Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication³.”

At the time of writing this report (October 2008), Austria had not implemented the directive in its Telecommunications Act and had been admonished by the EU Commission twice for not doing so. The Directive was realized in Germany on November 9, 2007 by passing the Act on Readjusting Telecommunications Surveillance.

In December 2007, the Social Democratic Party of Austria (SPÖ) and the Austrian Peoples Party (ÖVP) changed the Security Police Act (Sicherheitspolizeigesetz) so that all information and communication providers are required to pass on personal data of users, if the police ask for it. No judicial order is needed. In contrast to Austria, the German Federal Constitutional Court decided in March 2008 that providers only in the case of a judicial order and a severe criminal act must grant the police access to communication data.

Austrian Security Police Act §53 (3a):

“The security authorities have the right to demand from providers of public telecommunications services and other service providers the disclosure of:

1. Name, address, and identification number of a certain connection,
2. Internet protocol address (IP-address) of a specific message and the time of its transmission, as well as
3. Name and address of a user, to whom a certain IP address was allocated at a certain point of time,

if certain facts justify the assumption of a concrete threat and they require this data as an important precondition for the completion of the tasks that are assigned to them by this federal law. The identification of a connection according to point 1 can also take place by reference to a call taken via this connection through naming as precisely as possible a period of time and the passive user number for the completion of the general duty for first aid or the defence against dangerous attacks. The provider is required to disclose information immediately and at no charge⁴.”

² Data Retention Directive, Article 5, <http://www.ispai.ie/DR%20as%20published%20OJ%2013-04-06.pdf>, accessed on October 28, 2008.

³ Data Retention Directive, Article 6, <http://www.ispai.ie/DR%20as%20published%20OJ%2013-04-06.pdf>, accessed on October 28, 2008.

⁴ “§ 53 Sicherheitspolizeigesetz:

(3a) Die Sicherheitsbehörden sind berechtigt, von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 Telekommunikationsgesetz 2003 - TKG 2003, BGBl. I Nr. 70) und sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz - ECG, BGBl. I Nr. 152/2001) Auskunft zu verlangen über

1. Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses,
2. Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung sowie
3. Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation

In the surveillance society, the state is suspicious of individuals, everyone is suspected to be a potential criminal, the principle that you are not guilty before proven guilty seems to be reverted, one seems to be automatically suspected as being guilty as long as one cannot prove that one does not have criminal or terrorist intents. It is a society, where Guantanamo is not just a US military prison, but global society tends to become a Guantanamo society. This phenomenon has become increasingly pressing since September 11, 2001. Therefore one can assume that there are high pressure and expectations from states on providers to store all data for a certain amount of time and to provide access.

In the area of the economy, corporations are keen on knowing our consumption preferences for targeting us with personalized advertisements online. They do so either legally when you agree in an electronic contract to an analysis of your consumption preferences and to receive advertisements e.g. by e-mail or when you browse a web platform or illegally by sending spam mail or using invisible spyware that watches and transmits passwords and online behaviour.

For Marx, the profit rate is the relation of profit to investment costs: $p = s / (c + v)$. The investment costs are subdivided into constant and variable capital. Variable capital v is the value form of labour, constant capital c the value form of the means of production. The latter consists of two parts: circulating constant capital c_{cir} (the value of the utilized raw materials, auxiliary materials, operating supply items and semi-finished products) and fixed constant capital c_{fix} (the value of the utilised machines, buildings and equipment) (Marx 1885/1992, MEW 24: chapter 8). c_{cir} and v together form the circulating capital: They transfuse their value totally to the product and must be constantly renewed. c_{fix} remains fixed in the production process for many turnovers of the capital. Fixed constant capital decreases its value by each turnover of capital. Its value is decreased by Δc , which is a flexible value. Fixed constant capital like machinery does not create value and its value is never entirely transfused to capital at once. It is depreciated by wear and tear, non-usage, and moral depreciation (i.e. the emergence of new machinery with increased productivity) (Marx 1885/1992: 237f, MEW 24: 159).

In the production sphere, capital stops its metamorphosis; capital circulation comes to a halt. New value V' of the commodity is produced, V' contains the value of the necessary constant and variable capital and all surplus value of the surplus product. Surplus value is generated by unpaid labour. Corporations do not pay for the production of surplus, therefore the production of surplus value can be considered as a process of exploitation. The value V' of the commodity after production is $V' = c + v + s$. The commodity then leaves the production sphere and again enters the circulation sphere, where it is sold on the market, so that surplus value is transformed into profit. The value of the commodity is realized in money form. Parts of the profits are

rechtfertigen und sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen. Die Bezeichnung eines Anschlusses nach Z 1 kann für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder die Abwehr gefährlicher Angriffe auch durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer erfolgen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen“.

reinvested and capitalized in order to produce more profit. Capital is accumulated.

Commodities are sold at a price that is higher than the investment costs so that profit is generated. For Marx, the decisive quality of capital accumulation is that profit is an emergent property of production that is produced by labour, but owned by the capitalists. Without labour no profit could be made. Workers are forced to enter class relations and to produce profit in order to survive, which enables capital to appropriate surplus. The notion of exploited surplus value is the main concept of Marx's theory, by which he intends to show that capitalism is a class society.

The capitalist

“wants to produce a commodity greater in value than the sum of the values of the commodities used to produce it, namely the means of production and the labour-power he purchased with his good money on the open market. His aim is to produce not only a use-value, but a commodity; not only use-value, but a commodity; not only use-value, but value; and not just value, but also surplus-value. (...) The cotton originally bought for £100 is for example re-sold at £100 + £10, i.e. £110. The complete form of this process is therefore $M-C-M'$, where $M' = M + \Delta M$, i.e. the original sum advanced plus an increment. This increment or excess over the original value I call 'surplus-value'" (Marx 1867/1990: 293, 251; MEW 23: 201, 165).

The immediate effects of surplus-value production in class relations are that the product belongs to the capitalist and not to the worker and that surplus-value “costs the worker labour but the capitalist nothing, and (...) becomes the legitimate property of the capitalist” (Marx 1867/1990: 731, MEW 23: 611). If you do not produce cotton, but knowledge, such as for example the Microsoft Windows Vista operating system, the decisive quality is that knowledge only needs to be produced once and can be infinitely reproduced at low costs and distributed at high speed. There is no physical wear and tear of the product, knowledge is not used up in consumption, can be reworked and built upon. There are high initial production costs, but once knowledge as for example software is produced, it can be cheaply copied and sold at high prices. The constant and variable capital costs for reproduction are low, which is beneficial for sustained capital accumulation in the knowledge industries (Fuchs 2008).

The situation again changes a little if knowledge is produced for new media and carried and distributed by it. A central characteristic of networked digital media is that the consumer of knowledge has the potential to become its producer. Alvin Toffler (1980) spoke of the emergence of the prosumer within the information society. Axel Bruns applied this notion to new media and speaks of produsers – users become producers of digital knowledge and technology:

“Produsage, then, can be roughly defined as a mode of collaborative content creation which is led by users or at least crucially involves users as producers – where, in other words, Produsage, then, can be roughly defined as a mode of collaborative content creation which is led by users or at least crucially involves users as producers – where, in other words, the user acts as a hybrid user/producer, or produser, virtually throughout the production process” (Bruns

2007: 3f).

Philip Graham (2000) argues that hypercapitalism's immediacy and pervasiveness has resulted in the entanglement of production, circulation, consumption, material and non-material production, productive and unproductive labour, base and superstructure, forces and relations of production. Therefore value creation "becomes an immediate, continuous process" (Graham 2000: 137). New media are simultaneously used for the production, circulation, and consumption of knowledge. They support cognition (thought, language), communication (one-to-one, one-to-few, one-to-many, few-to-one, few-to-few, few-to-many, many-to-one, many-to-few, many-to-many), and co-operation (peer production, sharing, virtual communities, social networking, cyberlove, online collaboration, etc) by combining the universal digital machine of the computer with networking functions as structural principles (Fuchs 2008). In informational capitalism, the brain and its bodily mediations are enabled to engage in organic practices of economic production, surplus-value generation, co-production, communicative circulation, and productive consumption by new media. The production of knowledge is based on the prior consumption of the same, in co-production as well on communicative interchange as a coordinative mechanism. Consumption of knowledge produces individual meaning and incentives for further social production and communication. Circulation of knowledge is the consumption of bandwidth and technical resources and the production of connections.

If the users become productive, then in terms of Marxian class theory this means that they also produce surplus value and are exploited by capital as for Marx productive labour is labour generating surplus. Therefore the exploitation of surplus value in cases like Google, YouTube, MySpace, or Facebook is not merely accomplished by those who are employed by these corporations for programming, updating, and maintaining the soft- and hardware, performing marketing activities, and so on, but by wage labour and the producers who engage in the production of user-generated content. New media corporations do not (or hardly) pay the users for the production of content. One accumulation strategy is to give them free access to services and platforms, let them produce content, and to accumulate a large number of producers that is sold to third-party advertisers. Not a product is sold to the users, but the users are sold as a commodity to advertisers. The more users a platform has, the higher the advertising rates can be set. The productive labour time that is exploited by the capital on the one hand involves the labour time of the paid employees and on the other hand all of the time that is spent online by the users. For the first type of knowledge labour, new media corporations pay salaries. The second type of knowledge is produced completely for free. There are neither variable nor constant investment costs. The formula for the profit rate needs to be transformed for this accumulation strategy:

$p = s / (c + v_1 + v_2)$, s ... surplus value, c ... constant capital, v_1 ... wages paid to fixed employees, v_2 ... wages paid to users

The typical situation is that $v_2 \Rightarrow 0$ and that v_2 substitutes v_1 . If the production of content and the time spent online were carried out by paid employees, the variable costs would rise and profits would therefore decrease. This shows that produsage in a capitalist society can be interpreted as the outsourcing of productive labour to users who work completely for free and help maximizing the rate of exploitation ($e = s / v$) so

that profits can be raised and new media capital may be accumulated. This situation is one of infinite over-exploitation. Capitalist produsage is an extreme form of exploitation that the producers perform completely for free.

That surplus value generating labour is an emergent property of capitalist production means that production and accumulation will break down if this labour is withdrawn. It is the essential part of the capitalist production process. That producers conduct surplus-generating labour, can also be seen by imagining what would happen if they would stop using platforms like YouTube, MySpace, and Facebook: The number of users would drop, advertisers would stop investments because no objects for their advertising messages and therefore no potential customers for their products could be found, the profits of the new media corporations would drop and they would go bankrupt. If such activities were carried out on a large scale, a new economy crisis would arise. This thought experiment shows that users are essential for generating profit in the new media economy. Furthermore they produce and co-produce parts of the products, and therefore parts of the use value, exchange value, and surplus value that are objectified in these products.

Dallas Smythe (1981/2006) argues that in the case of media advertisement models, the audience is sold as a commodity:

“Because audience power is produced, sold, purchased and consumed, it commands a price and is a commodity. (...) You audience members contribute your unpaid work time and in exchange you receive the program material and the explicit advertisements” (Smythe 1981/2006: 233, 238).

With the rise of user-generated content and free access social networking platforms and other free access platforms that yield profit by online advertisement, the Web seems to come close to accumulation strategies employed by the capital on traditional mass media like TV or radio. The users who google data, upload or watch videos on YouTube, upload or browse personal images on Flickr, or accumulate friends with whom they exchange content or communicate online via social networking platforms like MySpace or Facebook, constitute an audience commodity that is sold to advertisers. The difference between the audience commodity on traditional mass media and on the Internet is that in the latter the users are also content producers; there is user-generated content, the users engage in permanent creative activity, communication, community building, and content-production. That the users are more active on the Internet than in the reception of TV or radio content is due to the decentralized structure of the Internet, which allows many-to-many communication. Due to the permanent activity of the recipients and their status as producers, I would, in the case of the Internet, argue that the audience commodity is a producer commodity. The category of the producer commodity does not signify a democratization of the media towards participatory systems, but the total commodification of human creativity. Much of the time spent online produces profit for large corporations like Google, News Corp. (which owns MySpace), or Yahoo! (which owns Flickr). Advertisements on the Internet are frequently personalized; this is made possible by surveilling, storing, and assessing user activities with the help of computers and databases. This is another difference from TV and radio, which provide less individualized content and advertisements due to their more centralized structure. But one can also observe a certain shift in the area of traditional

mass media, as in the cases of pay per view, tele-votes, talkshows, and call-in TV and radio shows. In the case of the Internet, the commodification of audience participation is easier to achieve than with other mass media.

Marx has anticipated the exploitation of producers by arguing that as a result of the development of the productive forces a time of capitalist development will come, in which “general intellect”, the “power of knowledge, objectified”, “general social knowledge has become a direct force of production” (Marx 1858/1993: 706, MEW 42: 602). The productive forces would not only be produced in the form of knowledge, but also as “immediate organs of social practice, of the real life process”. Marx here describes that in a knowledge society, social life becomes productive. That knowledge labour, such as the one performed online by producers, is productive, then also means that under capitalist class relations it is exploited and that all knowledge workers, unpaid and paid, are part of an exploited class.

The basic business models that dominate the Web are the advertising model, selling services to users, and combinations of the two (Fuchs 2008). That the first model is the dominant one can be seen from the fact that nine out of the ten most accessed Web platforms make use of it for accumulating capital:

1. Yahoo!,
2. Google,
3. YouTube,
- 4.+5. Windows Live Search and Microsoft Network (MSN),
6. Myspace,
8. Facebook,
9. Blogger,
10. Yahoo Japan

(Data from Alexa Global Top 500 (alexa.com), accessed on August 6, 2008). The only exception is Wikipedia (#7), which is non-profit oriented.

Figure 2 shows the rapid growth of Internet advertising profits in the USA. These profits amounted to 21.2 billion US\$ in 2007, which make up 11.0% of the total US advertising profits (Source: IAB Internet Advertising Revenue Report 2007). The online advertising profits were higher than the profits made by radio- and cable TV-advertising in 2007 and were only exceeded by profits in newspaper- and TV Distribution-advertising (Ibid.).

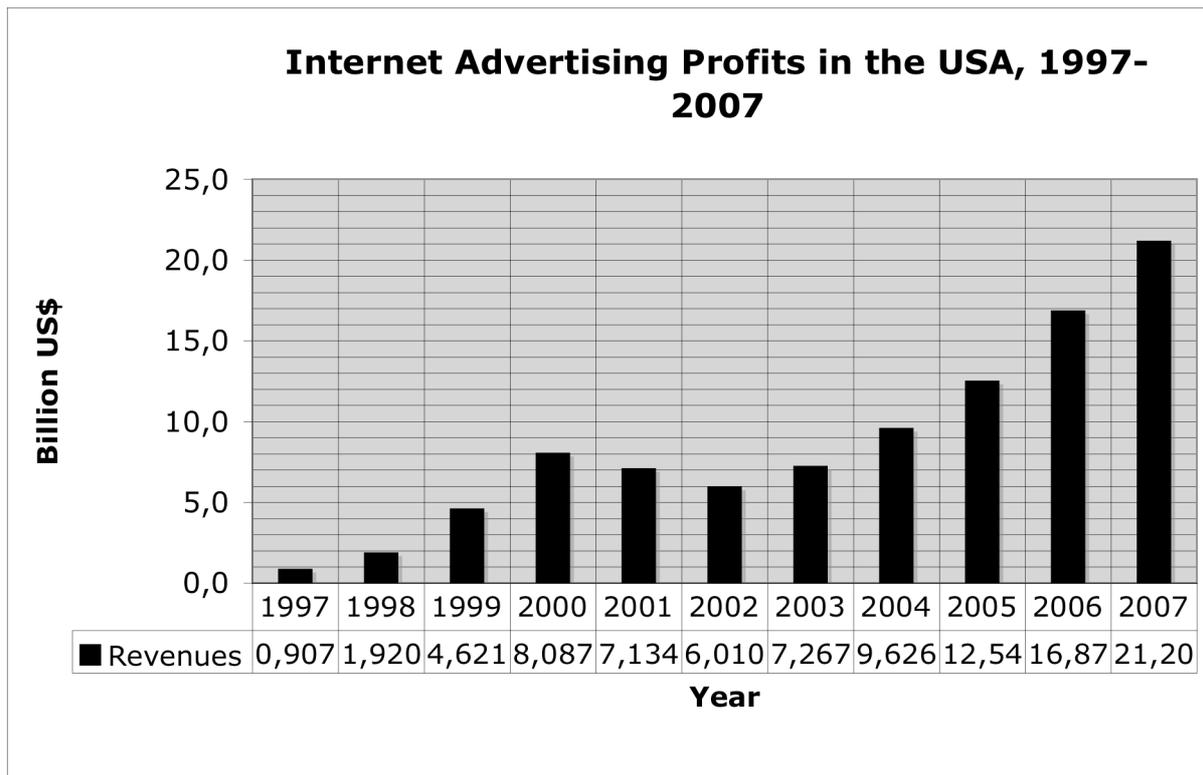


Figure 2. Internet advertising profits in the USA (Data Source: IAB Internet Advertising Revenue Report 2007)

The implications of these observations are manifold: New media companies generate profit by exploiting the labour of their users without paying them anything. In order to realize this profit (i.e. transforming surplus value into money capital), the collection, aggregation, assessment, and selling of data is necessary. As this collection serves instrumental economic reasons (profit maximization, money accumulation), we can speak of data collection that serves repressive economic goals. Therefore this is a form of economic surveillance.

This chapter intended to show that there are two major influences on the character of contemporary surveillance society: a political and an economic one. On the one hand, new imperialism has produced a situation, in which war and terror potentially reinforce each other, and the West reacts by increasing surveillance. This results in a contradiction between freedom and security and the short-sighted belief that more surveillance solves societal problems. On the other hand, not only the state, but also corporations have an interest in gathering personal data in order to develop personalized advertising strategies that target individual tastes and related tastes by aggregating and assessing user data.

Due to the ubiquity of the interest of the state and corporations in surveillance, users of ISNS are likely to be confronted by both.

5. Integrated Social Networking Sites: The Platforms in Our Study

Based on the theoretical foundations worked out in sections 1-4, the task is to research how students in Salzburg use ISNS in the context of economic and political surveillance. We have chosen three platforms that the study focuses upon: studiVZ, Facebook, MySpace. These platforms and their legal foundations will be introduced in this section.

5.1. studiVZ

studiVZ (studi=student, VZ=Verzeichnis, list, list of students) is an ISNS focusing on students as user group. It is primarily used in Germany and Austria. Ehsan Dariani and Dennis Bemmann formed the platform in October 2005. In January 2007, the German media corporation Holtzbrinck Networks purchased studiVZ for more than 50 million Euros. Holtzbrinck is a corporation that owns for example the publishing houses Fischer, Rowohlt, Macmillan, Scientific American, and publications such as Die Zeit, Der Tagesspiegel, or Nature. The corporation's profits were 206.6 million Euro in 2006⁵, which is a 10% annual increase in comparison to 2005. In December 2007, the terms of use of studiVZ were changed so that personalized advertisements became possible. Users can opt out of personalized ads, but the standard option is that they receive such ads. In September 2008, studiVZ was the fourth most visited website in Germany (158 583 022 visits⁶). It is ranked number 9 in the Alexa traffic rankings for Germany and number 14 for Austria (alexa.com, October 28, 2008). 86.6% of studiVZ users come from Germany, 7.6% from Austria⁷. The profits of studiVZ are not known, but one can imagine that they must be high given the advertising rates. So for example a coloured advertising wallpaper on the start page of all users costs 78 000 Euro per day⁸.

When registering, users must agree that studiVZ can store their usage behaviour, can send them emails and messages about news that concern studiVZ, can send up to five advertisement emails and messages per months to them, and that profile information is analyzed for providing personalized advertisements. The latter three points can be deactivated once one is registered by changing the privacy settings. This is an opt-out-and not an opt-in-process.

studiVZ does not define property and usage rights of content in its terms of use, therefore the users are the sole owners of the content that they post on their profiles.

The privacy policy of studiVZ states that users agree that usage data are saved for a maximum of six months: "I agree that information is transmitted automatically by my Internet browser if I access the studiVZ network and that it is stored for a period of six months at maximum in so-called protocol files (server log files)"⁹ (Privacy Policy §4).

⁵ Accessed on October 28, 2008.

⁶ IVW online usage data, <http://www.ivwonline.de/ausweisung2/search/ausweisung.php>, accessed on October 28, 2008).

⁷ http://www.alexa.com/data/details/traffic_details/studiverzeichnis.com (Accessed on October 28, 2008).

⁸ <http://www.gwp.de>, accessed on October 28, 2008.

⁹ "Ich willige ein, dass bei einem von mir veranlassten Zugriff auf das studiVZ-Netzwerk automatisch Informationen durch den von mir verwendeten Internet-Browser übermittelt und dass diese durch studiVZ für eine Zeitdauer von höchstens sechs Monaten in so genannten Protokolldateien (Server-

The users also agree that profile data and their clickstream are analyzed for being provided with personalized advertisements:

“I agree that studiVZ assesses and analyzes these so-called protocol files in order to optimize the studiVZ network and its applications as well as for presenting to me targeted personalized advertisements and/or special offers or services via the studiVZ network.

(...) The assessment of the so-called protocol files also includes analyses of the clickstream of the websites that comprise the studiVZ network in order to find out which areas of the studiVZ network have been visited how often and/or searched. In such a clickstream analysis, studiVZ can also use cookies and/or JavaScript in order to collect and assess information. Based on this agreement, advertisements and/or special offers and service, which are based on the information gained in connection with the clickstream-analyses (e.g. advertisement that is oriented on users that visit groups on a certain kind of sports), can be presented to the user through the studiVZ network” (Privacy policy, §4)¹⁰.

Users can opt out of personalized advertisements:

“I take notice that I can decline and disagree to the usage of my data, if I no longer wish to receive personalized advertisements. For doing so, I can access and adapt the settings on “options for the usage of my data” in the domain “data protection” at the end of the text of the agreement to the processing of personal data after successful login into the studiVZ network” (Privacy policy, §4)¹¹.

Profile data can be used for personalized advertisements. There is an opt-out from this option.

Logfiles) gespeichert werden” (Datenschutzerklärung §4).

¹⁰ “Ich erkläre mich damit einverstanden, dass studiVZ diese in den so genannten Protokolldateien gespeicherten Daten auswertet und analysiert, um das studiVZ-Netzwerk und seine Anwendungen zu optimieren sowie um mir gezielt personalisierte Werbung und/oder besondere Angebote und Services über das studiVZ-Netzwerk zu präsentieren bzw. präsentieren zu lassen. (...) Bei der Auswertung der so genannten Protokolldateien wird auch der Clickstream zu den, durch die und aus den Websites des studiVZ-Netzwerkes analysiert und dahingehend untersucht, welche Bereiche innerhalb des studiVZ-Netzwerkes wie oft aufgesucht und/oder gesucht werden. Bei einer solchen Clickstream-Analyse können durch studiVZ unter anderem auch Cookies und/oder JavaScript eingesetzt werden, um Informationen zu sammeln und zu bewerten. Dem Nutzer können so über das studiVZ-Netzwerk mit der erklärten Einwilligung Werbung und/oder besondere Angebote und Services präsentiert werden, deren Inhalt auf den im Zusammenhang mit der Clickstream-Analyse erlangten Informationen basiert (z.B. Werbung, die auf einen Nutzer ausgerichtet ist, der Gruppen zu einer bestimmten Sportart besucht)” (Datenschutzerklärung, §4, accessed on October 30, 2008).

¹¹ “Ich nehme zur Kenntnis, dass ich, falls eine solch personalisierte Werbung von mir nicht mehr erwünscht ist, diese ablehnen und der Nutzung meiner Daten jederzeit widersprechen kann. Hierzu kann ich nach dem erfolgreichen Einloggen in das studiVZ-Netzwerk in der Rubrik „Datenschutz“ am Ende des Textes zur Einwilligung in die Verarbeitung personenbezogener Daten meine Einstellungen unter ‘Einstellungen zur Verwendung meiner Daten’ aufrufen und anpassen” (Datenschutzerklärung, §4, accessed on October 30, 2008).

"I agree that studiVZ uses my registration data (e.g. gender and university, etc.), my voluntary submitted profile ("my page") data (e.g. study programme, interests, associations, musical style/bands, favourite books/films, etc.) as well as my group membership ("my groups") for presenting to me targeted personalized advertisements and/or special offers and services through the studiVZ network (e.g. a book recommendation that fits my study programme, ads for products that fit my interests, etc). I take notice that I can decline and disagree to the usage of my data, if I no longer wish to receive personalized advertisements. For doing so, I can access and adapt the settings on 'options for the usage of my data' in the domain 'data protection' at the end of the text of the agreement to the processing of personal data after successful login into the studiVZ network" (Privacy policy, §5)¹².

The users agree to receive advertising and technical messages per mail and message service, unless they opt out:

"I agree that studiVZ sends notifications and messages to me; these notifications contain references and reports for users of the studiVZ network. I notice that for doing so studiVZ uses my personal data depending on my selected settings; thus the sending takes place via email or the email address that I use for accessing the studiVZ network or via the message service.

I furthermore agree that studiVZ uses my personal data for sending me marketing messages per electronic mail (by sending emails to the email-address that I use for accessing the studiVZ network and/or by sending messages with advertising character to the message service of studiVZ).

I take notice that I can decline and disagree to receiving messages, if I no longer wish to receive electronic mail with advertising character. For doing so, I can access and adapt the settings on 'options for the usage of my data' in the domain 'data protection' at the end of the text of the agreement to the processing of personal data after successful login into the studiVZ network" (Privacy policy, §6)¹³.

¹² "Ich willige ein, dass studiVZ die von mir bei der Registrierung mitgeteilten Daten (z.B. Geschlecht und besuchte Hochschule etc.), die von mir freiwillig innerhalb meines eigenen Profils („Meine Seite“) eingetragenen Daten (z.B. Studiengang/-richtung, Interessen, Clubs/Vereine, Musikrichtung/Bands, Lieblingsbücher/-filme etc.) sowie meine Mitgliedschaft in Gruppen („Meine Gruppen“) dazu nutzt, um mir gezielt personalisierte Werbung und/oder besondere Angebote und Services über das studiVZ-Netzwerk zu präsentieren bzw. präsentieren zu lassen (z.B. eine auf meine(n) Studiengang/-richtung ausgerichtete Buch-empfehlung; Produktwerbung, die auf meinen Interessen beruht etc.).

Ich nehme zur Kenntnis, dass ich, falls eine solch personalisierte Werbung von mir nicht mehr erwünscht ist, diese ablehnen und der Nutzung meiner Daten jederzeit widersprechen kann. Hierzu kann ich nach dem erfolgreichen Einloggen in das studiVZ-Netzwerk in der Rubrik „Datenschutz“ am Ende des Textes zur Einwilligung in die Verarbeitung personenbezogener Daten meine Einstellungen unter „Einstellungen zur Verwendung meiner Daten“ aufrufen und anpassen" (Datenschutzerklärung, §5, accessed on October 30, 2008).

¹³ "Ich willige ein, dass mir studiVZ Benachrichtigungen und Mitteilungen zusendet; diese Nachrichten beinhalten Hinweise und Berichte für Nutzer des studiVZ-Netzwerkes. Ich nehme zur Kenntnis, dass studiVZ hierzu meine personenbezogenen Daten nach Maßgabe der von mir gewählten Einstellungen nutzt; demnach erfolgt die Zusendung per E-Mail an die von mir für die Nutzung des studiVZ-Netzwerkes verwendeten E-Mail-Adresse oder über den Nachrichtendienst.

Zudem erkläre ich mich einverstanden, dass studiVZ meine personenbezogenen Daten nutzt, um mir Marketing-Mitteilungen unter Verwendung elektronischer Post zuzusenden (zum Versand von E-Mails an

The users agree that their data are provided to the police if this is necessary for public safety or law enforcement:

“I agree that studiVZ passes my master data and/or usage data to inquiry authorities, law enforcement agencies, or state regulators, if and insofar this is necessary for the prevention of dangers for state and public security and for the prosecution of criminal offences” (Privacy policy, §7, accessed on October 30, 2008).

The privacy policy says that one can opt out of personalized advertisement and receiving ads per mail and message service, but that the usage behaviour of all members is stored:

“But please understand that we save the usage behaviour of all members, there is no alternative choice here. Reason and aim of the storage of usage data for a maximum of six month is the prevention and solving of cases of misuse and rights violations. The storage serves the security of our users and of our network. Our aim here is explicitly not the usage of data for economic goals (you can anyway limit this by the settings on the privacy page, see above), but to provide a secure and therefore attractive platform to our users. We want to offer the highest possible degree of safety and security to our users” (Privacy policy, §7)¹⁴.

This part of the privacy policy shows that not only economic surveillance, but also state surveillance is an important issue for studiVZ and that there are policy guidelines that allow economic surveillance, from which one can opt out, and state surveillance, from which one can not opt out. The storage of user data for six months reflects the EU's Data Retention Directive that has been implemented in Germany (studiVZ is a German legal entity).

die von mir für die Nutzung des studiVZ-Netzwerkes verwendete E-Mail-Adresse und/oder zum Versand von Nachrichten mit werbendem Charakter über den Nachrichtendienst von studiVZ). Ich nehme zur Kenntnis, dass ich, falls der Erhalt von elektronischer Post mit werbendem Charakter von mir nicht mehr erwünscht ist, die Zusendung ablehnen und dem Erhalt der Nachrichten jederzeit widersprechen kann. Hierzu kann ich nach dem erfolgreichen Einloggen in das studiVZ-Netzwerk in der Rubrik „Datenschutz“ am Ende des Textes zur Einwilligung in die Verarbeitung personenbezogener Daten meine Einstellungen unter „Einstellungen zur Verwendung meiner Daten“ aufrufen und anpassen” (Datenschutzerklärung, §6, accessed on October 30, 2008)

¹⁴ “Bitte habe aber Verständnis dafür, dass wir das Nutzerverhalten aller Mitglieder speichern, hier gibt es keine Wahlmöglichkeit. Sinn und Zweck der Speicherung der Nutzungsdaten für eine Höchstdauer von sechs Monaten ist die Vorbeugung und Aufklärung von Missbrauchsfällen und Rechtsverletzungen. Die Speicherung dient der Sicherheit unserer Nutzer und unseres Netzwerkes. Es geht uns hierbei ausdrücklich nicht um die Nutzung der Daten zu wirtschaftlichen Zwecken (dies kannst Du ja durch die Einstellungen auf der Privatsphäre-Seite ohnehin einschränken, siehe oben), sondern darum, den Mitgliedern eine sichere und deshalb attraktive Plattform zu bieten. Wir möchten unseren Nutzern das größtmögliche Maß an Schutz und Sicherheit gewähren” (Datenschutzrichtlinie, §7, accessed on October 30, 2008).

5.2. Facebook

Mark Zuckerberg founded Facebook in February 2004. Microsoft purchased 1.6% of Facebook for more than 240 million US\$ in October 2007. Other than MySpace, Facebook is based on local university and city networks. In terms of Internet traffic, Facebook is ranked number five at the global level, number 16 in Germany, number 11 in Austria, and number 4 in Switzerland (alexa.com, accessed on October 28, 2008). The three-month average share of global Internet users who use Facebook is 10.41% (alexa.com, accessed on October 28, 2008). In 2007, MySpace had more unique visitors than Facebook, but in 2008 Facebook outstripped MySpace (unique visitors of Facebook in June 2008: 132 million, MySpace: 117 million¹⁵) and became the largest ISNS. The number of unique visitors increased by 153% in the period from June 2007 to June 2008 (June 2007: 52 million)¹⁶. Facebook makes profits of approximately 10-50 million US\$ per year¹⁷. It is a legal entity in the USA.

In November 2007, Facebook started the Beacon advertising system. This system collects usage data on other partner websites, even if the user is logged out from Facebook, and uses this data for personalized and social advertising (targeting a group of friends) on Facebook. The partner sites include for example eBay, LiveJournal, New York Times, Sony, STA Travel, or TripAdvisor. Users can opt out from this service, but it is automatically activated and legalized by Facebook's privacy policy:

"Facebook Beacon is a means of sharing actions you have taken on third party sites, such as when you make a purchase or post a review, with your friends on Facebook. In order to provide you as a Facebook user with clear disclosure of the activity information being collected on third party sites and potentially shared with your friends on Facebook, we collect certain information from that site and present it to you after you have completed an action on that site. You have the choice to have Facebook discard that information, or to share it with your friends" (Facebook Privacy Policy, accessed on November 2, 2008).

By signing up to Facebook, users agree to its terms of use and thereby grant the company a license for using and selling all content that is uploaded to the platform:

"When you post User Content to the Site, you authorize and direct us to make such copies thereof as we deem necessary in order to facilitate the posting and storage of the User Content on the Site. By posting User Content to any part of the Site, you automatically grant, and you represent and warrant that you have the right to grant, to the Company an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to use, copy, publicly perform, publicly display, reformat, translate, excerpt (in whole or in part) and distribute such User Content for any purpose, commercial, advertising, or otherwise, on or in connection with the Site or the promotion thereof, to prepare derivative works of, or incorporate into other works, such User Content, and to grant and authorize sublicenses of the foregoing. You may remove

¹⁵ <http://www.comscore.com/press/release.asp?press=2396>, accessed on October 28, 2008.

¹⁶ <http://www.comscore.com/press/release.asp?press=2396>, accessed on October 28, 2008.

¹⁷ <http://www.alexa.com/data/details/main/facebook.com>, accessed on October 28, 2008.

your User Content from the Site at any time. If you choose to remove your User Content, the license granted above will automatically expire, however you acknowledge that the Company may retain archived copies of your User Content. Facebook does not assert any ownership over your User Content; rather, as between us and you, subject to the rights granted to us in these Terms, you retain full ownership of all of your User Content and any intellectual property rights or other proprietary rights associated with your User Content" (Facebook Terms of Use, accessed on November 2, 2008).

Facebook stores personal data and usage data. These data are also used for personalized services.

"When you visit Facebook you provide us with two types of information: personal information you knowingly choose to disclose that is collected by us and Web Site use information collected by us as you interact with our Web Site. (...) When you use Facebook, you may set up your personal profile, form relationships, send messages, perform searches and queries, form groups, set up events, add applications, and transmit information through various channels. We collect this information so that we can provide you the service and offer personalized features. In most cases, we retain it so that, for instance, you can return to view prior messages you have sent or easily see your friend list. When you update information, we usually keep a backup copy of the prior version for a reasonable period of time to enable reversion to the prior version of that information" (Facebook Privacy Policy, accessed on November 2, 2008).

Facebook automatically uses targeted advertising. There is no way to opt out.

"Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as aggregating how many people in a network like a band or movie and personalizing advertisements and promotions so that we can provide you Facebook. We believe this benefits you. You can know more about the world around you and, where there are advertisements, they're more likely to be interesting to you. For example, if you put a favorite movie in your profile, we might serve you an advertisement highlighting a screening of a similar one in your town. But we don't tell the movie company who you are. (...) Advertisements that appear on Facebook are sometimes delivered (or "served") directly to users by third party advertisers. They automatically receive your IP address when this happens. These third party advertisers may also download cookies to your computer, or use other technologies such as JavaScript and "web beacons" (also known as "1x1 gifs") to measure the effectiveness of their ads and to personalize advertising content. Doing this allows the advertising network to recognize your computer each time they send you an advertisement in order to measure the effectiveness of their ads and to personalize advertising content. In this way, they may compile information about where individuals using your computer or browser saw their advertisements and determine which advertisements are clicked. Facebook does not have access to or control of the cookies that may be placed by the third party advertisers. Third party advertisers have no access to your contact information stored on Facebook unless you choose to share it with them. This privacy policy covers the

use of cookies by Facebook and does not cover the use of cookies or other tracking technologies by any of its advertisers” (Facebook Privacy Policy, accessed on November 2, 2008).

Facebook is allowed to automatically collect information on users from other websites and to publish these data on the users’ Facebook profiles:

“We may use information about you that we collect from other sources, including but not limited to newspapers and Internet sources such as blogs, instant messaging services, Facebook Platform developers and other users of Facebook, to supplement your profile. Where such information is used, we generally allow you to specify in your privacy settings that you do not want this to be done or to take other actions that limit the connection of this information to your profile (e.g., removing photo tag links)” (Facebook Privacy Policy, accessed on November 2, 2008).

Facebook is allowed to share user data with its advertising clients:

“We may offer stores or provide services jointly with other companies on Facebook. You can tell when another company is involved in any store or service provided on Facebook, and we may share customer information with that company in connection with your use of that store or service” (Facebook Privacy Policy, accessed on November 2, 2008).

Facebook may pass on data to authorities for crime prevention or law enforcement:

“We may be required to disclose user information pursuant to lawful requests, such as subpoenas or court orders, or in compliance with applicable laws. We do not reveal information until we have a good faith belief that an information request by law enforcement or private litigants meets applicable legal standards. Additionally, we may share account or other information when we believe it is necessary to comply with law, to protect our interests or property, to prevent fraud or other illegal activity perpetrated through the Facebook service or using the Facebook name, or to prevent imminent bodily harm. This may include sharing information with other companies, lawyers, agents or government agencies” (Facebook Privacy Policy, accessed on November 2, 2008).

5.3. MySpace

Tom Anderson, Josh Berman, Chris DeWolfe, and Brad Greenspan launched MySpace in August 2003. MySpace was purchased by Rupert Murdoch’s News Corporation for 580 million US\$ in July 2005. News Corporation was the 136th largest company in the world in 2008 (Forbes 2000 list of largest companies, 2008) and the fourth largest media corporation. Its profits amounted to 3.33 billion US\$ in 2007, its capital assets were 30.55 billion US\$. News Corporation owns for example newspapers such as The Sun, The New York Post, The Wall Street Journal; the film production company 20th Century Fox, the TV stations FOX in the US and ITV in the UK. MySpace is especially important for bands and music fans because it allows musicians to upload six mp3s to their profiles. In terms of Internet traffic, MySpace is ranked number 7 at the global

level, number 14 in Germany, number 12 in Austria, and number 18 in Switzerland (alexa.com, accessed on October 29, 2008). The three-month average share of global Internet users who use MySpace is 6.49% (alexa.com, accessed on October 28, 2008). In 2007, MySpace had more unique visitors than Facebook, but in 2008 Facebook outstripped MySpace (unique visitors of MySpace in June 2008: 117 million, Facebook: 132 million¹⁸) and MySpace no longer was the largest ISNS. The number of unique MySpace visitors increased by 3% in the period from June 2007 to June 2008 (June 2007: 114 million)¹⁹. Facebook makes profits of approximately 250-500 million US\$ per year²⁰.

In summer 2006, British socialist folk singer Billy Bragg discussed publicly that MySpace's terms of use allow them to sell and reuse artists' songs that are uploaded to MySpace. The specific passage read:

"You hereby grant to MySpace.com a non-exclusive, fully-paid and royalty-free, worldwide license (with the right to sublicense through unlimited levels of sublicensees) to use, copy, modify, adapt, translate, publicly perform, publicly display, store, reproduce, transmit, and distribute such Content on and through the Services".

MySpace reacted and amended the specific passage so that reuse and reselling is not allowed:

"MySpace does not claim any ownership rights in the text, files, images, photos, video, sounds, musical works, works of authorship, applications, or any other materials (collectively, 'Content') that you post on or through the MySpace Services. After posting your Content to the MySpace Services, you continue to retain any such rights that you may have in your Content, subject to the limited license herein. By displaying or publishing ('posting') any Content on or through the MySpace Services, you hereby grant to MySpace a limited license to use, modify, delete from, add to, publicly perform, publicly display, reproduce, and distribute such Content solely on or through the MySpace Services, including without limitation distributing part or all of the MySpace Website in any media formats and through any media channels, except Content marked 'private' will not be distributed outside the MySpace Website. This limited license does not grant MySpace the right to sell or otherwise distribute your Content outside of the MySpace Services. After you remove your Content from the MySpace Website we will cease distribution as soon as practicable, and at such time when distribution ceases, the license will terminate. If after we have distributed your Content outside the MySpace Website you change the Content's privacy setting to "private," we will cease distribution of such 'private' Content outside the MySpace Website as soon as practicable after you make the change" (MySpace Terms of Use, §6.1, accessed on November 3, 2008).

¹⁸ <http://www.comscore.com/press/release.asp?press=2396>, accessed on October 28, 2008.

¹⁹ <http://www.comscore.com/press/release.asp?press=2396>, accessed on October 28, 2008.

²⁰ <http://www.alexa.com/data/details/main/myspace.com>, accessed on October 28, 2008.

MySpace collects

“personally identifiable information (“PII”-- your full name, email address, mailing address, telephone number, or credit card number). (...) In addition, MySpace collects other non-PII including IP address, aggregate user data, and browser type. This data is used to manage and improve the MySpace Services, track usage, and for security purposes” (MySpace Privacy Policy, accessed on November 3, 2008).

MySpace allows targeted personalized advertising that is automatically activated. Users can opt out, but doing so is very difficult. There is no menu setting in the privacy options that allows doing so, only a link in the privacy policy that users have to follow in order to opt out.

“MySpace may use cookies and similar tools to customize the content and advertising you receive based on the Profile Information you have provided. Profile Information you provide in structured profile fields or questions (multiple choice questions like ‘Marital Status,’ ‘Education’ and ‘Children’) (‘Structured Profile Information’), information you add to open-ended profile fields and questions (essay questions like ‘About Me,’ ‘Interests’ and ‘Movies’) (‘Non-Structured Profile Information’) and other non-PII about you may also be used to customize the online ads you encounter to those we believe are aligned with your interests. For example, based on your music interests we might display an advertisement to make sure you are advised when your favorite band is coming to town. The information used for this feature does not provide your PII or identify you as an individual to third parties. If you would like to disable advertising customization for Non-Structured Profile Information, please log in and click here” (MySpace Privacy Policy, accessed on November 3, 2008).

Third party advertisers are allowed to collect information from profiles. Users can opt out, but again doing so is very complicated and only possible by following a link in the privacy policy.

“Some of the advertisements that appear on MySpace Services may also be delivered to you by third party Internet advertising companies. These companies utilize certain technologies to deliver advertisements and marketing messages and to collect non-PII about your visit to or use of MySpace Services, including information about the ads they display, via a cookie placed on your computer that reads your IP address. To opt out of information collection by these companies, or to obtain information about the technologies they use or their own privacy policies, please click here” (MySpace Privacy Policy, accessed on November 3, 2008).

MySpace may share personal information, such as email addresses, with advertising clients for “business reasons”. This means that in such cases companies are allowed to send advertising messages per email to MySpace users.

“MySpace may also provide your PII to a third party in those instances where you have chosen to receive certain information and have been notified that the fulfillment of such a request requires the sharing of your PII. MySpace also may

share your PII with Affiliated Companies if it has a business reason to do so. As described in ‘Notice’ above, MySpace may customize the advertising and marketing messages you receive on the MySpace Website, or may work with outside companies to do so. Your non-PII and/or Profile Information may be shared with these companies so this customization can be accomplished. MySpace prohibits these companies from sharing your non-PII and/or Profile Information with any third party or from using it for any other purpose. Anonymous click stream, number of page views calculated by pixel tags, and aggregated demographic information may also be shared with MySpace’s advertisers and business partners” (MySpace Privacy Policy, accessed on November 3, 2008).

MySpace is allowed to disclose personal information of its users to law enforcement agencies:

“There may be instances when MySpace may access or disclose PII, Profile Information or non-PII without providing you a choice in order to: (i) protect or defend the legal rights or property of MySpace, our Affiliated Companies or their employees, agents and contractors (including enforcement of our agreements); (ii) protect the safety and security of Users of the MySpace Services or members of the public including acting in urgent circumstances; (iii) protect against fraud or for risk management purposes; or (iv) comply with the law or legal process. In addition, if MySpace sells all or part of its business or makes a sale or transfer of all or a material part of its assets or is otherwise involved in a merger or transfer of all or a material part of its business, MySpace may transfer your PII to the party or parties involved in the transaction as part of that transaction” (MySpace Privacy Policy, accessed on November 3, 2008).

5.4. ISNS as Platforms of Economic and Political Surveillance

	studiVZ	Facebook	MySpace
Selling and reuse of user content is allowed		X	
Targeted personalized advertising is allowed	X (opt out)	X (no opt out)	X (opt out)
Sharing of data with third parties is allowed for commercial aims		X (no opt out)	X (opt out)
Reception of advertising emails is allowed	X (opt out)	X	X
Passing on of data to the police for law enforcement or crime prevention	X	X	X

Table 3. Rights guaranteed to corporations by terms of use and privacy policies on studiVZ, Facebook, and MySpace

Table 3 summarizes the most important rights that are granted by the terms of use and privacy policies to the three integrated social networking platforms that have just been discussed. Facebook is the platform that makes use of intellectual property rights and data surveillance most extensively. It does not even have opt out options for targeted advertising. There are opt out mechanisms for social ads and beacons, which are specific forms of targeted advertising, but not for such ads in general. MySpace and studiVZ do not have the right to resell user content. MySpace has opt out options for targeted advertising and the sharing of data with advertising clients for commercial

aims. But these options are so hidden that one can expect that only few people will find them and deactivate them. studiVZ is the only of the three platforms that does not share data with third parties and that allows to opt out of advertising emails. All three platforms pass data on to the police if it is necessary for law enforcement. In some of the privacy policies, the myth that surveillance guarantees security is reinforced. So for example studiVZ speaks of the need of surveillance in order to guarantee “prevention of dangers for state and public security and (...) the prosecution of criminal offences”. MySpace wants to “protect the safety and security of Users of the MySpace Services or members of the public including acting in urgent circumstances” with the help of surveillance.

Overall, this overview shows that commercial social networking platforms have an economic interest in collecting, assessing, and selling data and share the political attitude of surveillance for public security. Targeted personalized advertising is a standard feature of all three platforms. It is no accident that this is not an opt-in solution because if this were the case, less user behaviour data could be collected and sold to advertising clients, which would have negative influences on profits. Therefore we can conclude that corporate ISNS have a profit interest in economic surveillance. They are also willing to share the myth of surveillance as security, which is realized in privacy policies that state that personal data might be given to government authorities. In the age of post-9/11, nation states are eager to collect data on citizens because they think this is a way to prevent potential terrorism. Therefore such privacy policies by ISNS not only advance the security myth, but also support the rise of a surveillance society, in which all citizens are considered as potential criminals and terrorists and fundamental freedoms are limited. We can conclude that from a critical perspective the most important feature of ISNS considered at the level of society as totality is not that they enable communication and networking, which are only interpersonal, but not societal features, but that they are online platforms that enforce economic and political surveillance and ideological myths of a secure society that is achieved by advancing surveillance.

6. Integrated Social Networking Sites (ISNS): Research Method

Specific research that has been conducted on ISNS include: appearance and attractiveness on Facebook (Tom Tong et al. 2008, Walther et al. 2008), business and policy implications of SNS and other “participatory Web and user-generated content” (OECD 2007), effects of MySpace and YouTube on election campaigns (Gueorguieva 2008), factors that influence privacy settings (Lewis/Kaufman/Christiakis 2008), friendship (boyd 2006a), gender (Magnuson/Dundes 2008, Cohen/Shade 2008), implications for libraries (Charnigo/Barnett-Ellis 2007, Harris/Lessick 2007), language use (Carroll 2008, Herring et al. 2007), media theory (Beer 2006), medical education (Ferdig et al. 2008, McGee/Begg 2008, Thompson et al. 2008), music culture (Baym 2007, Beer 2008a), pharmacy education (Cain 2008), place and identity (Goodings/Locke/Brown 2007), psychological distress (Baker/Moore 2008), research ethics (Moreno/Fost/Christakis 2008), self-esteem and sociability (Zywica/Danowski 2008), SNS as virtual learning environments (Mitchell/Watstein 2007) and their role in education (Mazer/Murphy/Simonds 2007), studies of specific users such as African Americans (Byrne 2007) or the Korean site Cyworld (Kim and Yun 2007, Haddon and Kim 2007), taste performance (Liu 2007), teenage life (boyd 2008b), the blurring of publicness and privatness (Lange 2007), the rise of marketing relationships on ISNS as challenge for public relations (Meadows-Klues 2008), or work skills (Bernardo 2007).

Corporate and state surveillance has thus far not been an issue in ISNS research. Most specific studies operate on the micro level of analysis and do not focus on the critique of coercive and repressive totalities, i.e. macro contexts. Therefore our study is different from most other studies that have thus far been carried out because it focuses on how economic and political macro contexts shape ISNS and it critically analyzes and questions these influences.

We conducted an empirical case study on the relationship of surveillance society and ISNS usage by students in Salzburg. The research was carried out from October to December 2008. The questionnaire was available for 50 days to the students. The basic research questions were:

- (1) What do students consider as the greatest opportunities of ISNS?
- (2) What do students consider as the greatest risks of ISNS?
- (3) How knowledgeable are students of the rise of a surveillance society?
- (4) How critical are students of the rise of a surveillance society?
- (5) How does the degree of knowledge about surveillance and the degree of critical consciousness on surveillance influence the usage of social networking sites?

We constructed a questionnaire that consisted of 35 (single and multiple) choice questions, 3 open-ended questions, and 5 interval-scaled questions. The questionnaire was implemented as an electronic survey with the help of the online tool Survey Monkey. Our potential respondents were students in Salzburg. In order to reach them, we sent out invitations to participate with the help of the University of Salzburg’s eLearning platform Blackboard, we asked local online platforms that are frequently used by students in Salzburg to post invitations to their platforms and to send out newsletters (<http://www.unihelp.cc>, <http://www.salzburg24.at>, <http://www.where2be.at>, <http://www.salzblog.at>). We also posted invitations to all discussion groups on studiVZ,

Facebook, and MySpace that have to do with students' life in Salzburg. These were in total 53 groups. We distributed flyers and hanged up posters at Salzburg's three universities: Paris Lodron University of Salzburg (Faculty of Humanities and Social Sciences, Faculty of Natural Sciences, Faculty of Law, Faculty of Theology), Mozarteum Salzburg: The University of Music, Theatre and Visual Arts, Paracelsus Medical University. An invitation to participate in the survey was sent as part of a newsletter to all students at the University of Salzburg on November 18, 2008. As an incentive for participation, we gave away three Amazon vouchers (60€, 25€, 25€) among those who completed the survey.

In order to answer the first two research questions, we asked the students what they considered as the greatest advantages and risks of ISNS and if they have further comments on such platforms. This allows us to conduct a quantifying qualitative analysis of the answers given.

The socio-demographic variables included: gender, age, status at university (undergraduate student, graduate student, doctoral student, etc), number of completed semesters, faculty, income, urban/rural-origin, educational status of parents, class origin, usage frequency of ISNS.

Knowledge of surveillance society and policies was measured with the help of an index (surveillance knowledge index) that was calculated based on the answers given to three questions that tested such knowledge. For each correct answer, one point was given so that zero points indicated a low knowledge, one point a modest knowledge, two points a medium knowledge, and three points a good knowledge of surveillance.

(17)

Web platforms in Austria have to pass on personal data (name, email-address, etc) to the police:

Yes, always if the police demands so (X)

No, never

Only if the policy has a juridical order that was passed by a court and is handed over to the provider.

(18)

Platforms such as studiVZ, Facebook, or MySpace store data about me only as long as I do not delete my account.

Yes, this is correct.

No, this is incorrect (X).

(19)

I can describe in one sentence exactly what the Data Retention Directive is:

Yes

No

X...correct answer

The first question tests students' knowledge of the Austrian Security Policy Act. The second question tests knowledge about data storage. The third question assesses students' knowledge of the European Data Retention Directive.

How critical students are of surveillance, i.e. if they consider surveillance as an actual

problem or hardly think of it as a problem, was assessed with an index that we constructed based on the results of five interval-scaled questions.

	1	2	3	4	5	6
(20) If you have nothing illegal to hide, then you need not be afraid of surveillance.						
(21) I trust that social networking platforms such as studiVZ, MySpace, or Facebook deal in a responsible way with my data.						
(22) In Austria, there are only few laws that allow the surveillance of Internet and phone communication. Citizens are therefore well protected from state surveillance.						
(23) Firms have a strong interest in gathering personal data of Internet users.						
(24) State surveillance of citizens has increased after the terrorist attacks in New York on September 11, 2001.						

1...I completely disagree, 6...I fully agree

Table 4. Questions on which the surveillance critique index is based

The index can be calculated by the following formula:

$$\text{Surveillance Critique Index} = (6 - \text{value}(20)) + (6 - \text{value}(21)) + (6 - \text{value}(22)) + \text{value}(23) - 1 + \text{value}(24) - 1$$

0-5: uncritical of surveillance society

6-10: hardly critical of surveillance society

11-15: modest criticism of surveillance society

16-20: rather critical of surveillance society

21-25: critical of surveillance society

For answering research questions 3 and 4, we can make use of the results obtained for the surveillance knowledge index and the surveillance critique index.

For each of the three relevant ISNS (studiVZ, Facebook, MySpace), we asked questions about students' knowledge of privacy policy and terms of use as well as their advertising settings. For answering research question 5, the socio-demographic factors, the surveillance knowledge index, and the critique of surveillance index are correlated with the knowledge about privacy policy and terms of use and with the advertising settings. These correlations are carried out separately for each of the three platforms.

7. Results

7.1. General Characteristics of the Respondents

702 respondents participated in the survey. 28 datasets were deleted from the dataset because the respondents indicated that they were no students or former students and the study focuses on academic usage of SNS. The remaining N=674 datasets were analyzed. There were 67.5% female and 32.5% male respondents. This reflects very well the overall gender distribution of students in Salzburg. At the University of Salzburg, which accounts by far for the largest amount of students in Salzburg, there were 63.3% female and 36.7% male students in 2006²¹.

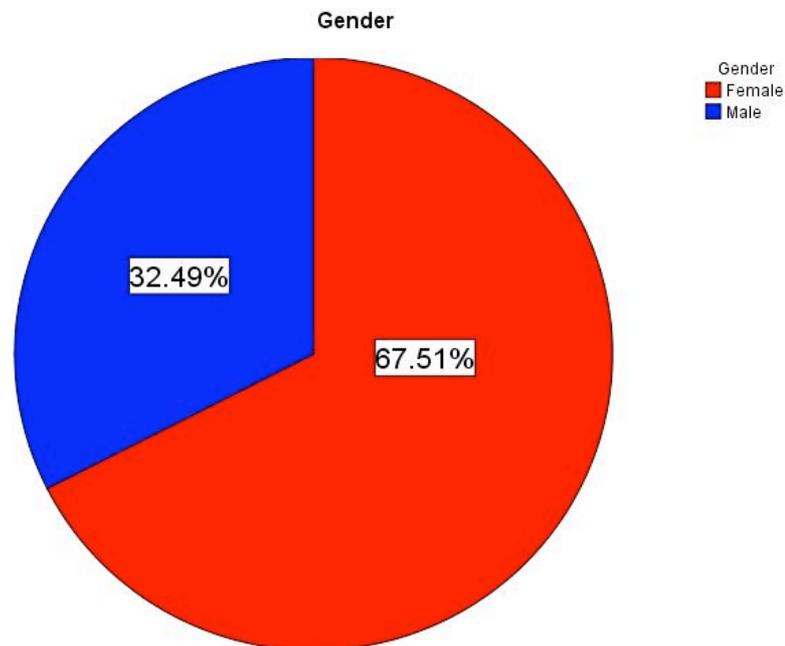


Figure 3. Gender distribution of the data

The mean age of our respondents was 24.16 years, the mean number of studied semesters 6.4. The sample was dominated by undergraduate and graduate students (figure 4), which accounted in total for more than 87% of all respondents.

²¹ University of Salzburg, Wissensbilanz 2006, http://www.unisalzburg.at/pls/portal/docs/PAGE/DIEUNIVERSITAET/SN_LI_VORSTELLUNG/WISSENSBILANZ_2006.PDF, accessed on December 2, 2008.

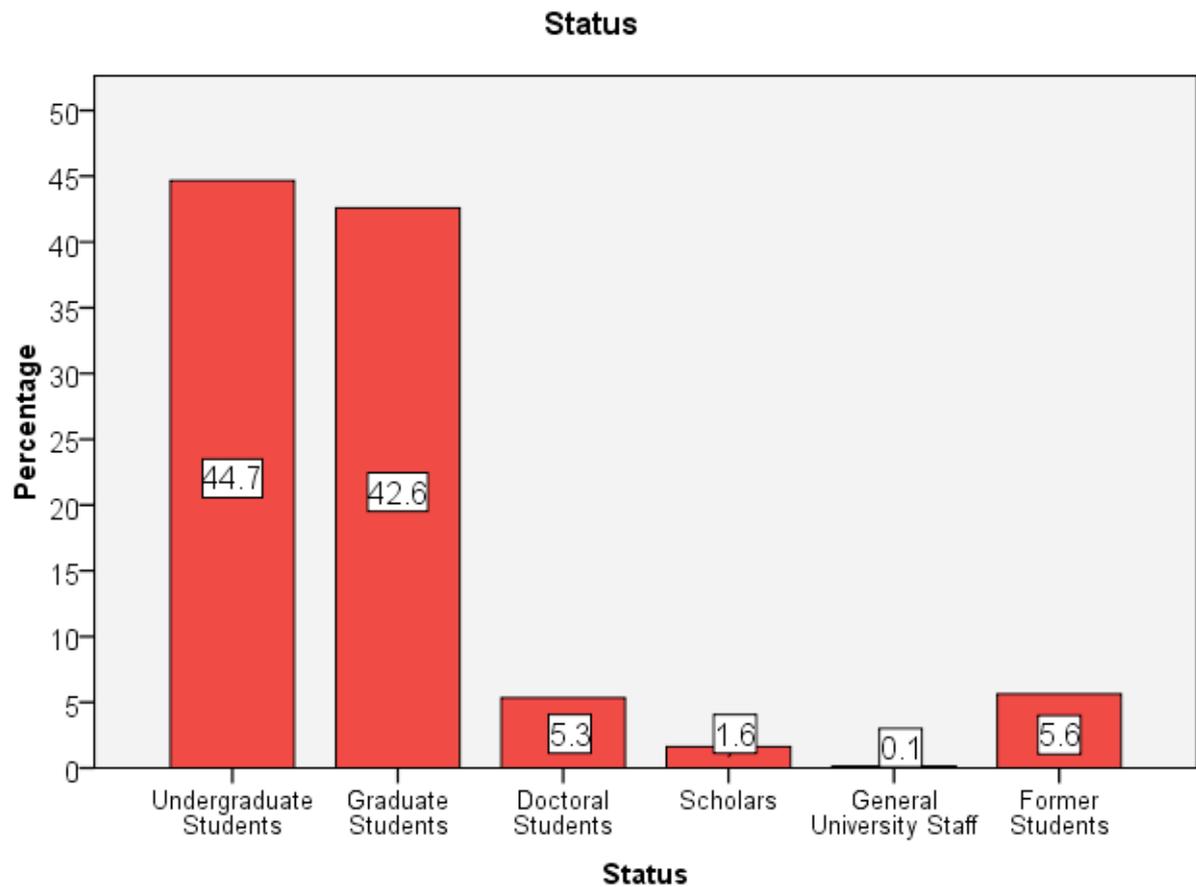


Figure 4. Status of respondents

Field of Study	Share in sample (N=656)	Share in Salzburg (N=15532, 2006/2007)
Social Sciences and Humanities	61.7%	48.5%
Natural and Engineering Sciences	26.0%	24.5%
Fine Arts	2.3%	8.3%
Sports Science		
Medical Science	0.8%	1.4%
Law	9.1%	17.4%

Table 5. Representation of different fields of study

Table 5 shows the representation of fields of study in our sample data and Salzburg's Universities (University of Salzburg²², Mozarteum²³, PMU²⁴).

²² <http://www.uni-salzburg.at/pls/portal/docs/1/515540.PDF> (Accessed on December 2, 2008).

²³ <https://mozonline.moz.ac.at/mozonline/StudierendenStatistik.html> (Accessed on December 2, 2008).

²⁴ Wikipedia, accessed on December 2, 2008.

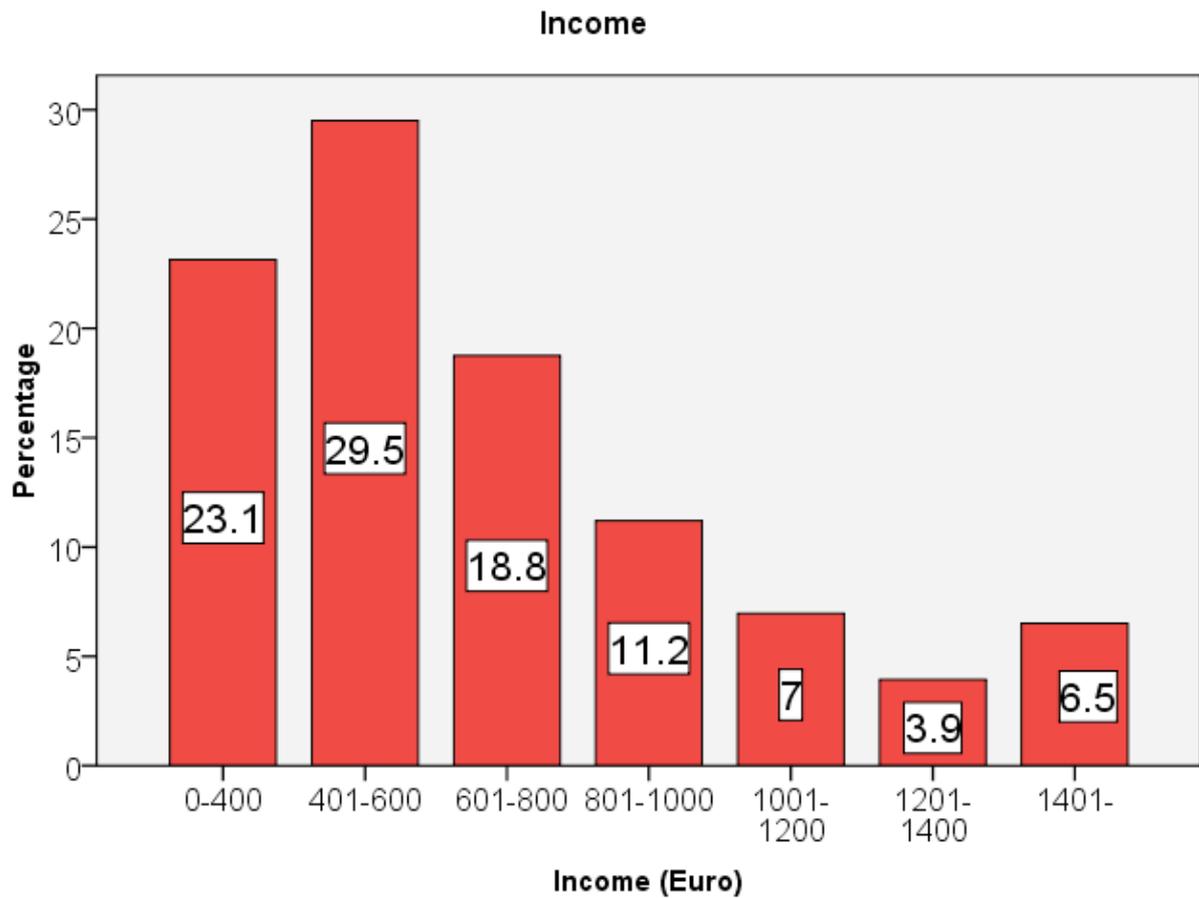


Figure 5. Income of respondents

52.6% of the respondents earn less than 600 € per month (figure 5). 37.8% have lived in towns with less than 5000 inhabitants, 63.0% in towns with less than 20 000 inhabitants, for most of their lifetime (figure 6).

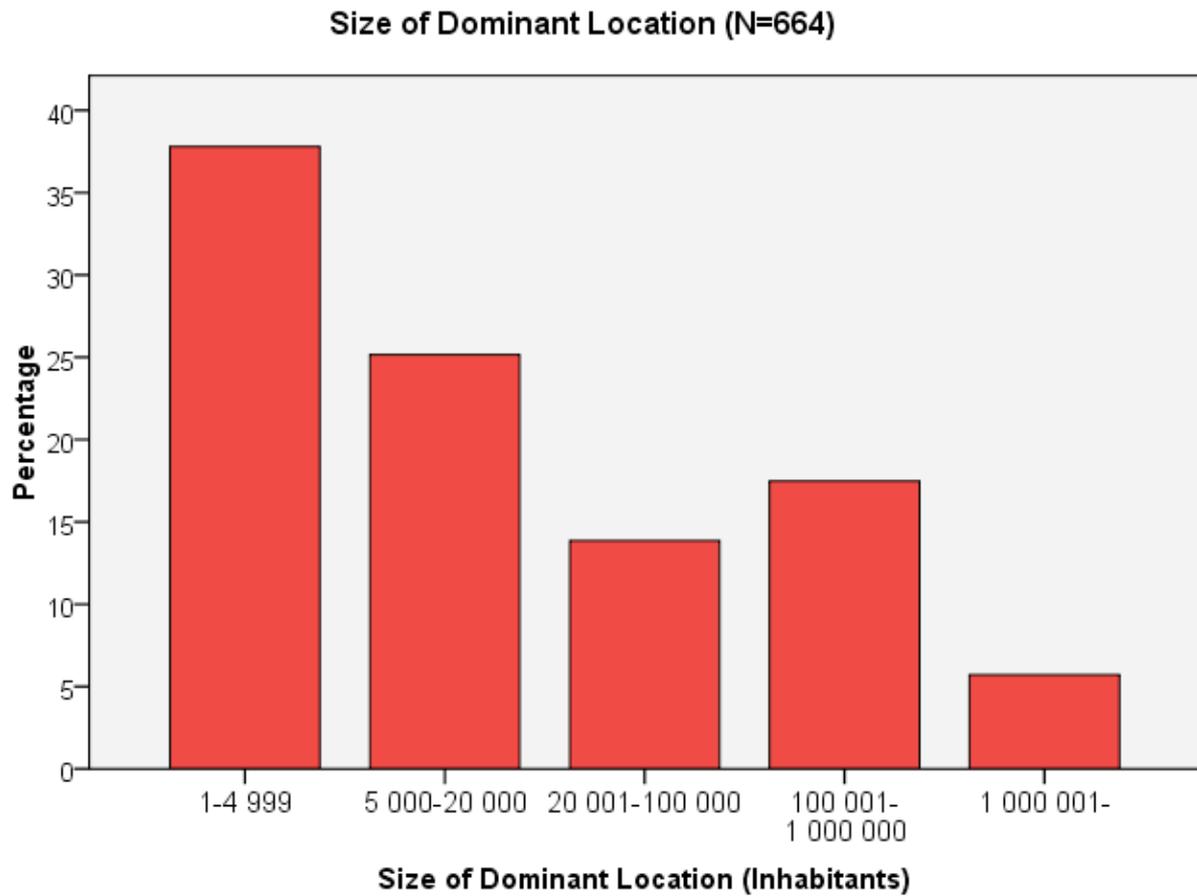


Figure 6. Size of city that respondents have lived in for most of their lifetime

65.5% of the respondents' parents have completed compulsory school or obtained school leaving examination as highest educational achievement (figure 7). The predominant occupation of the respondents' fathers and mothers is white-collar employment (figure 8, 9).

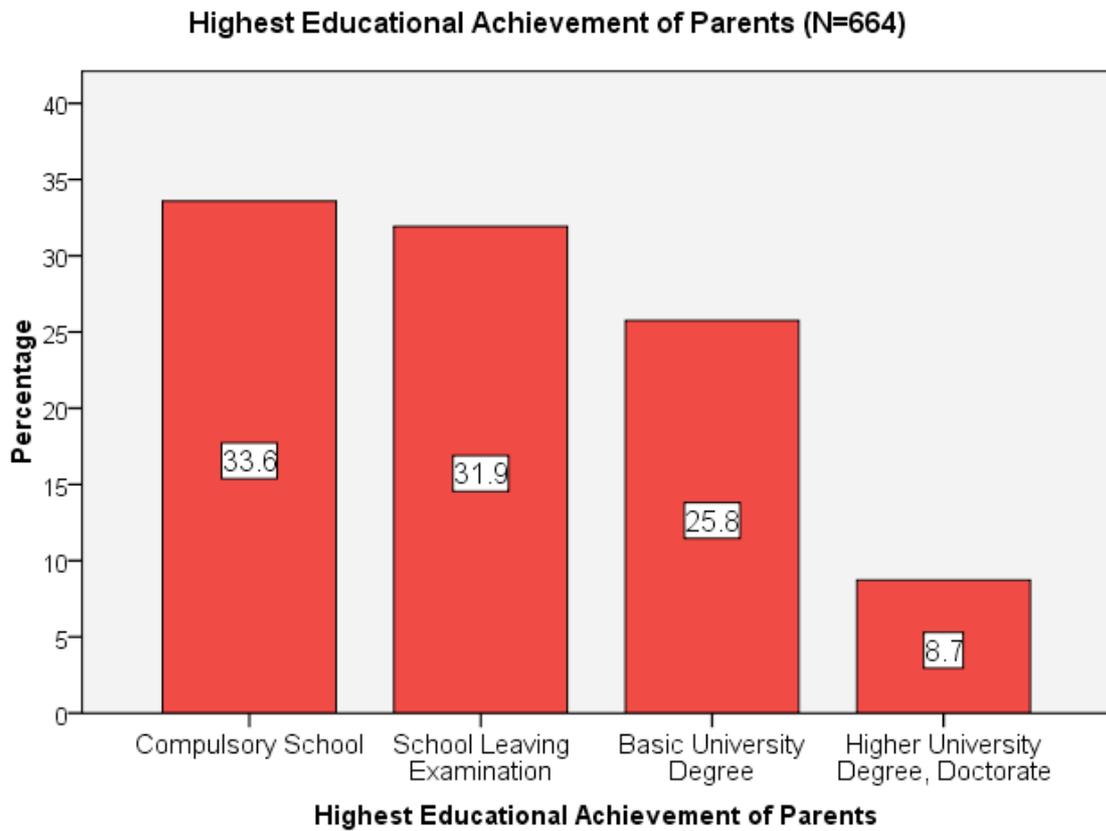


Figure 7. Highest educational achievement of respondents' parents

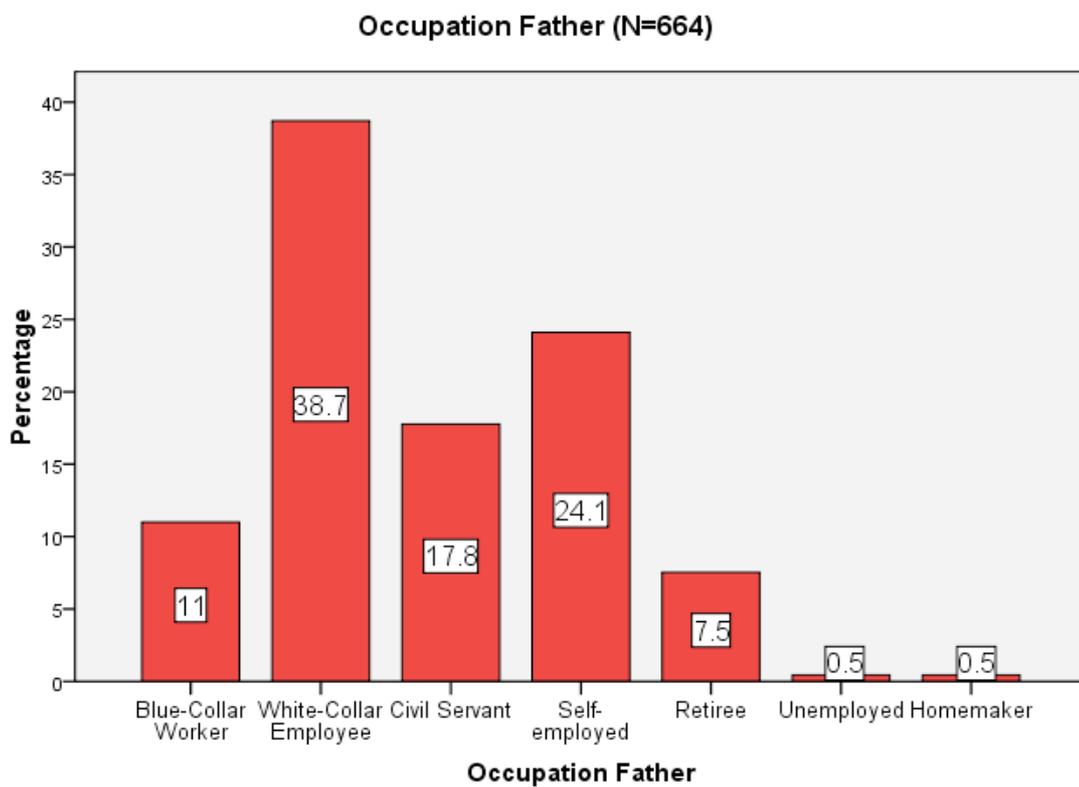


Figure 8. Occupation of respondents' fathers

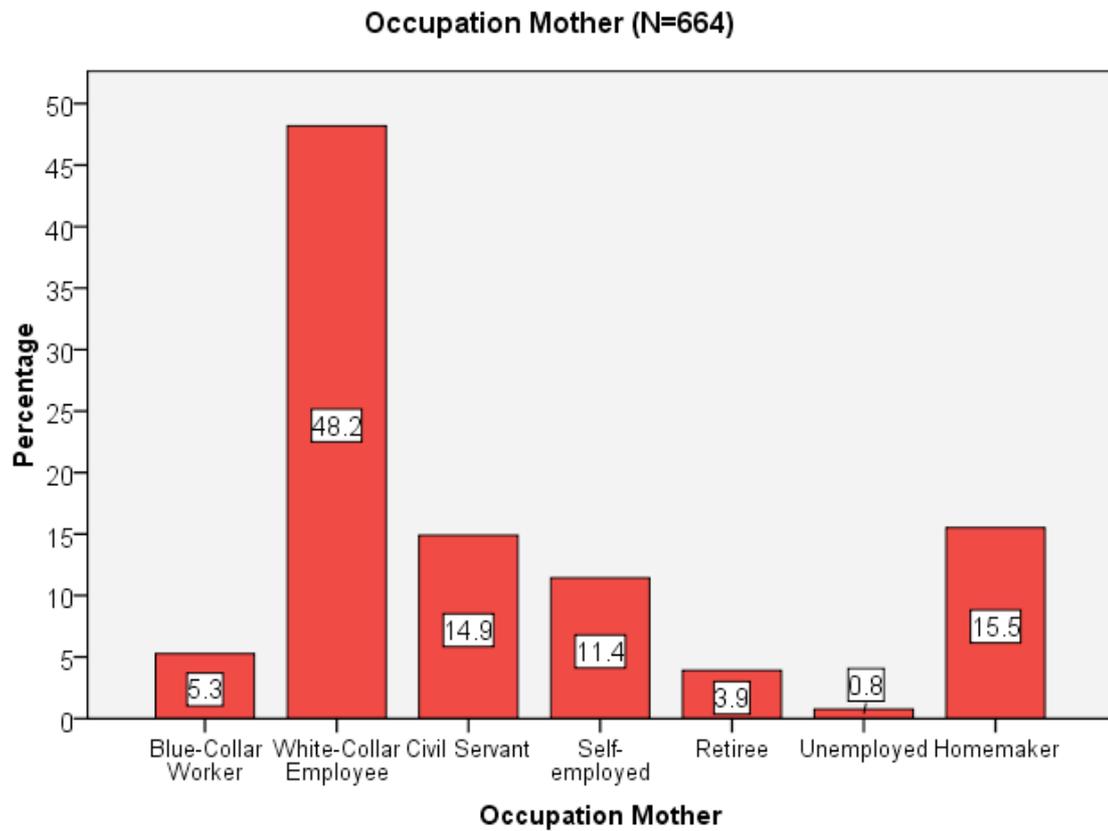


Figure 9. Occupation of respondents' mothers

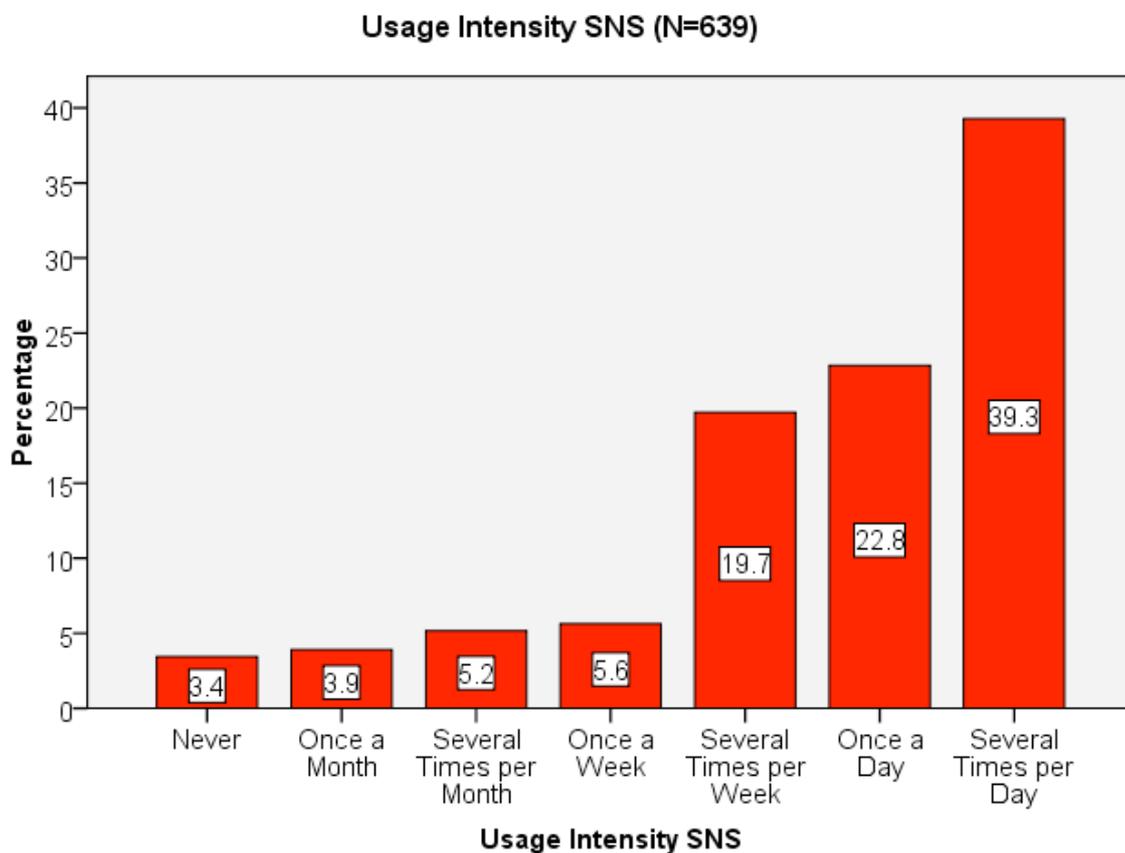


Figure 10. Usage intensity of integrated social networking platforms

Most of the respondents are heavy users of integrated social networking sites (ISNS). 39.3% use such platforms several times per day, 22.8% once a day (figure 10). So 62.1% of the respondents use ISNS at least once a day. This is an indication that these platforms have become very popular among students in Salzburg in particular, and Austrian students in general. Only 3.4% of the respondents never use such platforms, which is an indication that students are highly e-literate/e-educated and value online communication. 49.5% of the respondents read the terms of use of ISNS never or superficially; only 13.9% read them almost entirely or completely (figure 11). This shows that information behaviour concerning interest in what Internet companies are allowed to do with user data is rather small. We do not think that users are to blame for this fact, but that rather the providers are to blame because terms of use are normally very long, difficult to read, and do not allow objections by the users (they cannot influence the text of the terms of use and can only agree or disagree).

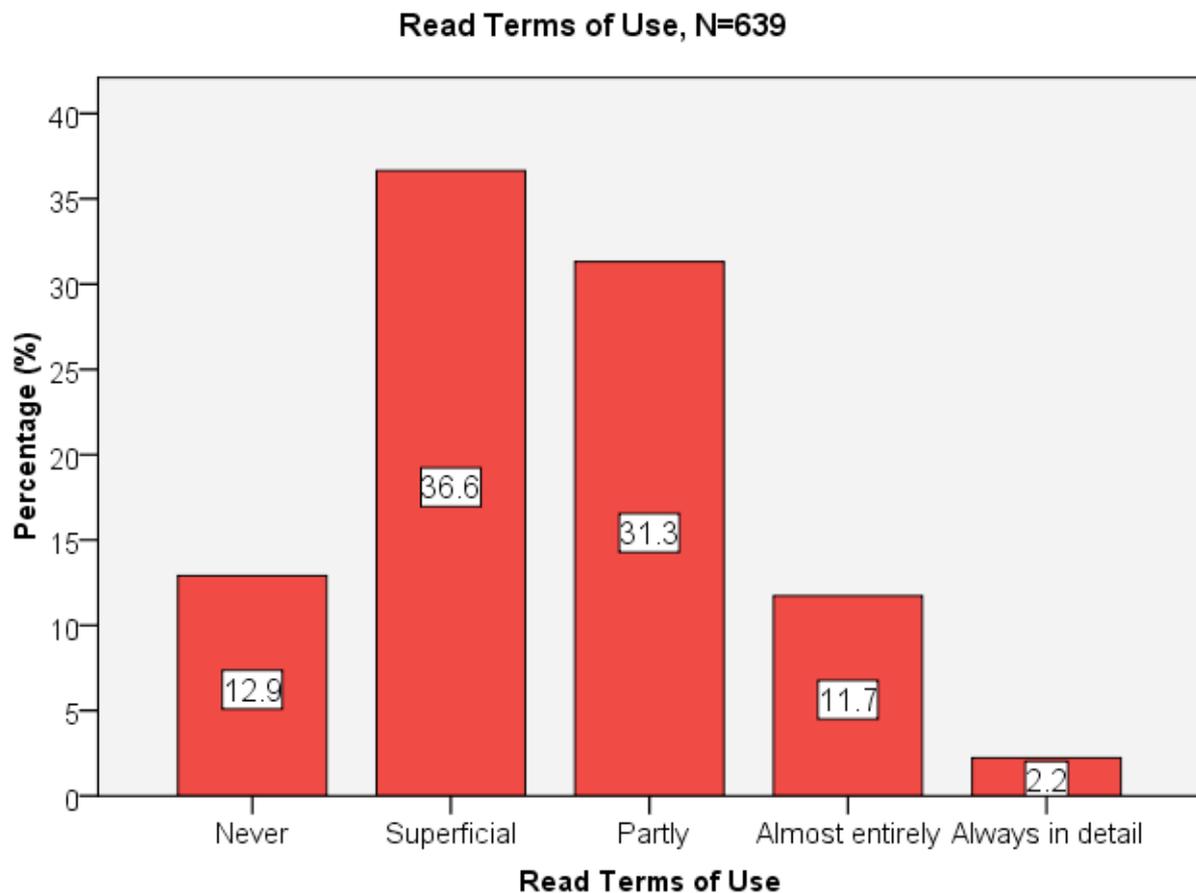


Figure 11. Intensity of reading the terms of use

7.2. Surveillance Knowledge

The next four figures show that our respondents had little knowledge of surveillance in Austria and Europe. Only 8.9% chose the right answer in the first instance and only 15.7% of the respondents said that they know what data retention (in German: Vorratsdatenspeicherung) is. However, 79.2% of the respondents knew or guessed right that many social networking platforms store certain data even after accounts have been deactivated by the users. This could be an indication that Austrian students know more

about surveillance if it immediately concerns technologies that they use very frequently than about general policies that set legal conditions for surveillance. studiVZ in its privacy policy says that it stores protocol data up to six months (§4), even after a profile has been deleted. In its terms of use, studiVZ specifies that it deletes account data and personal information of users as soon as a profile has been deactivated. The Facebook privacy policy says that data can be stored for an unspecified amount of time after users have deactivated their profiles. MySpace's privacy policy says that MySpace continues to store personally identifiable information (name, email, address, phone number, credit card number) after profile deletion for judicial reasons. This shows that to various degrees user data are stored after profiles are deleted. Although there are differences in degree, all three platforms that are relevant for this study store some data about users after they have deactivated their profiles. By combining the answers to all three questions to one surveillance knowledge index, one sees that 16.5% (0 correct answers) of the respondents have no, 65.3% (1 correct answer) little, 16.5% (2 correct answers) average, and 1.8% (3 correct answers) high knowledge of surveillance (figure 15). The median of the surveillance knowledge index is 1 (little knowledge of surveillance).

Surveillance Knowledge 1: Web platforms in Austria have to pass on personal data (name, email-address, etc) to the police (N=626)

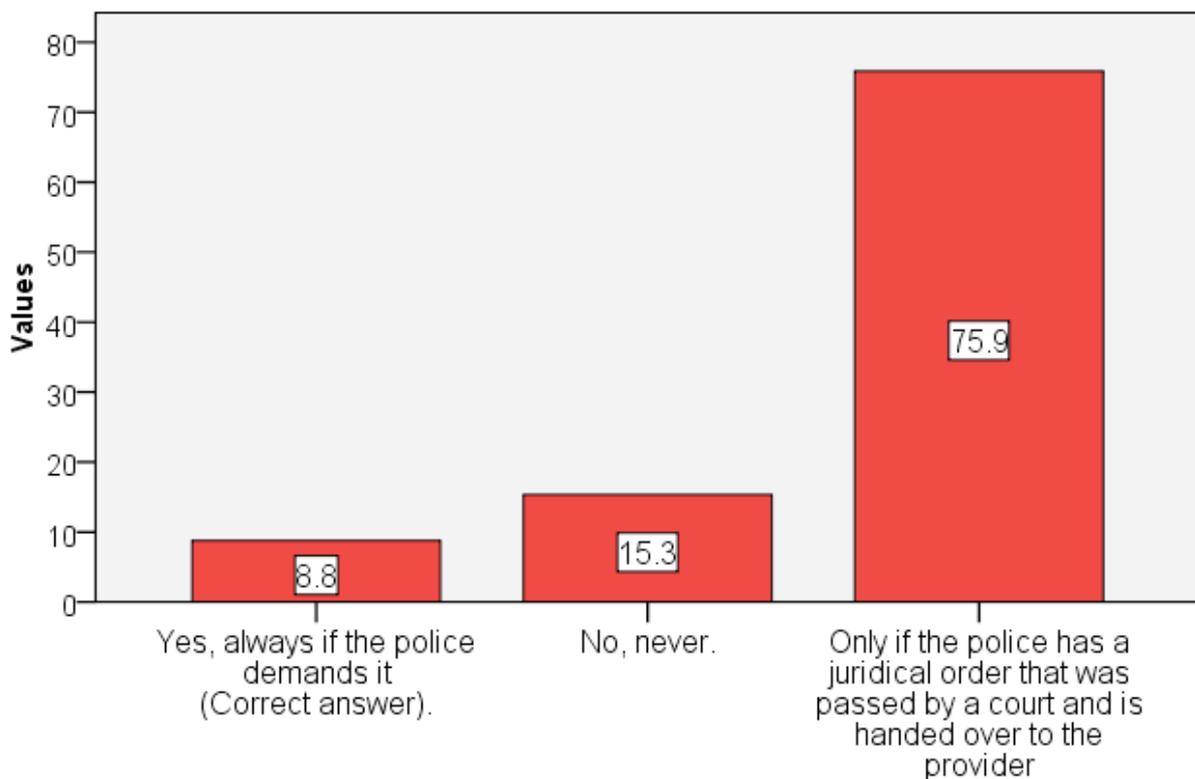


Figure 12. Knowledge of surveillance #1

Surveillance Knowledge 2: Platforms as studiVZ store my data only as long until I delete them and not any longer (N=626).

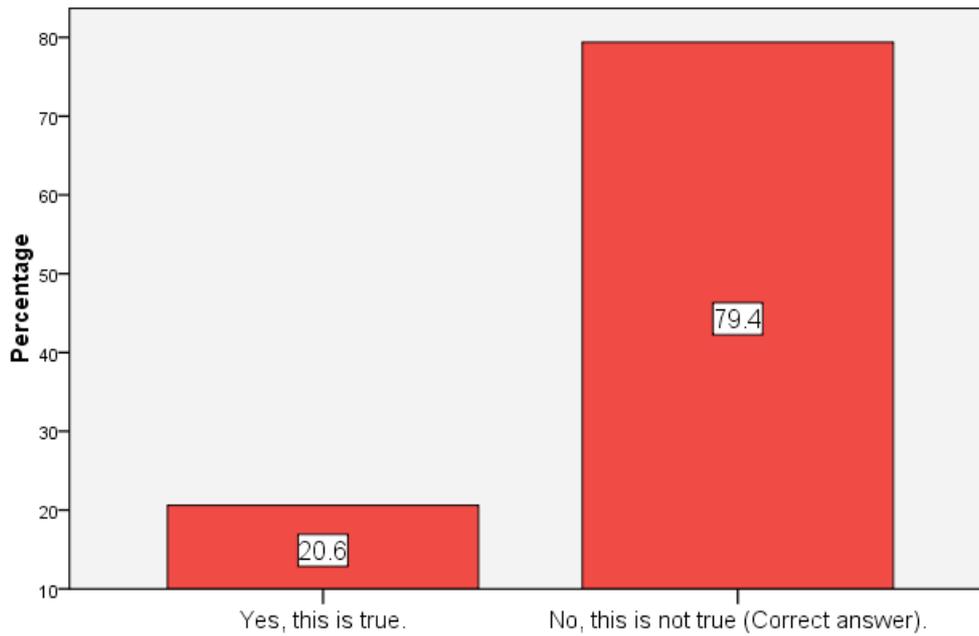


Figure 13. Knowledge of surveillance #2

Surveillance knowledge 3: I can describe in one sentence exactly what the Data Retention Directive is (N=626).

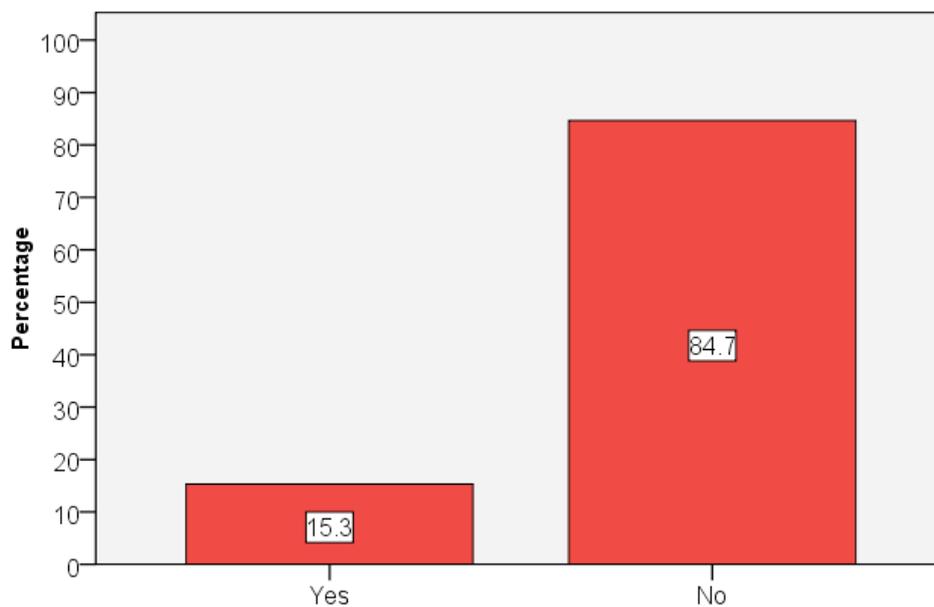


Figure 14. Knowledge of surveillance #3

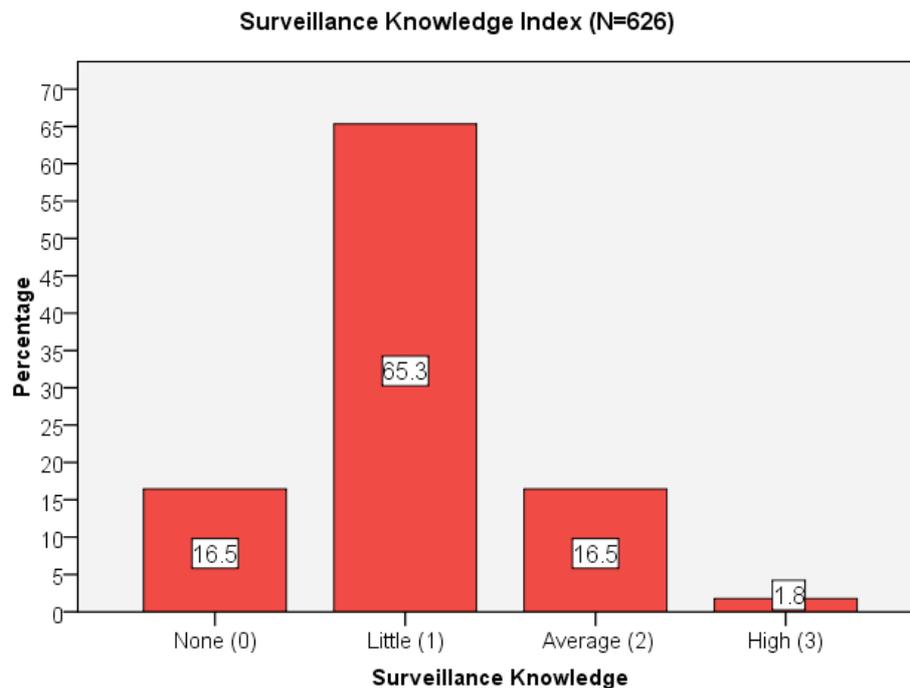


Figure 15. Surveillance knowledge index (one point for each correct answers to the questions shown in figures 12-14)

Table 6 shows bivariate correlations between the surveillance knowledge index and other factors. The result is that the surveillance knowledge index is significantly (at the 0.01 level) negatively correlated to female gender (positively to male gender) and the white-collar status of a student's father. It is significantly (at the 0.01 level) positively correlated to the status of a student's father as househusband, income, and the size of the location that the students have been living in for most of their lifetime. This means that being female decreases the possibility of high surveillance knowledge, whereas being a man increases it. This result could reflect dominant patriarchal values that construct men as powerful, rational, and knowledgeable and women as weak, irrational, and unknowing. If the father of a student is a white-collar worker, then the likelihood of high surveillance knowledge decreases. One reason that one can imagine is that as these fathers are all dealing with information in their jobs and work in offices, they could have a more positive attitude towards information processing and data surveillance than most blue-collar workers because data gathering is an everyday routine for them. It could be that a certain amount of these white-collar workers passes on their attitude towards data gathering to their kids. Another result, that might at a first glance rather seem obscure, is that if a student's father's job is to be a househusband, then the likelihood that the student has higher surveillance knowledge increases. However, given the still predominant patriarchal family relations, it is clear that in most conservative families, fathers are wageworkers and mothers either housewives or housewives and wageworkers. Therefore it is likely that families, where fathers are househusbands, are more liberal families. Liberal attitudes are normally more critical of state interference into privacy than conservative ones. In Austria, this can be observed for example by the fact that conservatives tend to oppose gay marriage and argue for a superiority of heterosexual marriage that should be guaranteed by the state. Liberal family climates could therefore explain a certain increase of the likelihood to have high

surveillance knowledge in those cases where students have househusbands as fathers. Students with higher income have a higher probability to have high surveillance knowledge. This can be explained by the fact that more money enables students to access better education facilities, more and therefore also more diverse information sources and cultural activities. Coming from a larger city increases the probability that one has more knowledge of surveillance. This can be explained by the difference in cultural infrastructure between urban and rural areas. Rural areas tend to be culturally more homogenous than urban areas, which normally are more culturally diverse. A lack of cultural infrastructure also means a lack of diversity of available worldviews, potential experiences, and viewpoints. Therefore it is more likely that people in larger cities are confronted with viewpoints (either in personal conversations or in the media or in cultural institutions) that are not present in rural areas and that they have access to more diverse information sources. The analysis shows overall that gender and class and the urban/rural-differential are three factors that influence surveillance knowledge.

	Surveillance Knowledge Index
Female: Correlation Coefficient Sig. (2-tailed) N	-0.203** 0.000 561
Male: Correlation Coefficient Sig. (2-tailed) N	0.203** 0.000 561
Age: Correlation Coefficient Sig. (2-tailed) N	0.087 0.030 626
Undergraduate Student: Correlation Coefficient Sig. (2-tailed) N	0.017 0.671 626
Graduate Student: Correlation Coefficient Sig. (2-tailed) N	-0.084 0.036 626
Doctoral Student: Correlation Coefficient Sig. (2-tailed) N	0.059 0.143 626
Semesters: Correlation Coefficient Sig. (2-tailed) N	0.037 0.362 614
Social Sciences, Humanities: Correlation Coefficient Sig. (2-tailed) N	0.046 0.253 614
Natural Sciences: Correlation Coefficient Sig. (2-tailed) N	-0.069 0.086 614
Engineering Sciences: Correlation Coefficient Sig. (2-tailed)	0.032 0.428

N	614
Fine Arts: Correlation Coefficient Sig. (2-tailed) N	-0.062 0.125 614
Sports: Correlation Coefficient Sig. (2-tailed) N	-0.046 0.257 614
Medical Science: Correlation Coefficient Sig. (2-tailed) N	0.067 0.097 614
Law: Correlation Coefficient Sig. (2-tailed) N	0.033 0.408 614
Income: Correlation Coefficient Sig. (2-tailed) N	0.135** 0.001 623
Size of Dominant Location: Correlation Coefficient Sig. (2-tailed) N	0.115** 0.004 626
Highest Educational Achievement of Parents: Correlation Coefficient Sig. (2-tailed) N	0.068 0.087 626
Father Blue Collar Worker: Correlation Coefficient Sig. (2-tailed) N	0.014 0.730 626
Father White Collar Worker: Correlation Coefficient Sig. (2-tailed) N	-0.108** 0.007 626
Father Civil Servant: Correlation Coefficient Sig. (2-tailed) N	0.030 0.456 626
Father Self-Employed: Correlation Coefficient Sig. (2-tailed) N	0.048 0.231 626
Father Retiree: Correlation Coefficient Sig. (2-tailed) N	0.022 0.581 626
Father Unemployed: Correlation Coefficient Sig. (2-tailed) N	0.036 0.364 626
Father Househusband: Correlation Coefficient Sig. (2-tailed) N	0.114** 0.004 626

Mother Blue Collar Worker: Correlation Coefficient Sig. (2-tailed) N	0.026 0.512 626
Mother White Collar Worker: Correlation Coefficient Sig. (2-tailed) N	-0.023 0.560 626
Mother Civil Servant: Correlation Coefficient Sig. (2-tailed) N	-0.012 0.770 626
Mother Self-Employed: Correlation Coefficient Sig. (2-tailed) N	0.035 0.387 626
Mother Retiree: Correlation Coefficient Sig. (2-tailed) N	-0.034 0.390 626
Mother Unemployed: Correlation Coefficient Sig. (2-tailed) N	0.057 0.154 626
Mother Housewife: Correlation Coefficient Sig. (2-tailed) N	0.002 0.970 626
Usage Intensity ISNS: Correlation Coefficient Sig. (2-tailed) N	-0.032 0.424 626
Read Terms of Use: Correlation Coefficient Sig. (2-tailed) N	0.100 0.012 626
** Correlation is significant at the 0.01 level (2-tailed)	

Table 6. Bivariate correlations of surveillance knowledge index and other factors

7.3. Critique of Surveillance

The next five tables report the results of scaled questions that aimed at assessing how critical and sensitive students are towards surveillance issues. Overall, the students in our study have a rather high degree of critical sensitivity towards surveillance. 71.8% disagree (to a certain extent) to the statement that one need not be afraid of surveillance if one has nothing to hide. 53% disagree (to a certain extent) to the statement that social networking platforms can be trusted in how they deal with private data. 73.2% disagree (to a certain extent) that Austrians are well protected from state surveillance. 87.0% agree or agree strongly that corporations have a strong interest in gathering personal data. 58.9% agree (to a certain extent) that state surveillance has increased after 9/11.

If we combine the answers to these five questions to an overall index (surveillance critique index, for the definition of this index see table 4), then the statistical average of this index is 17.3 (scale: 0-25, 0=no critique towards surveillance, 25=high level of

critique towards surveillance) (N=613). This indicates a rather critical stance of the students in our sample towards surveillance as problem. The exact distribution is shown in figure 16. 67.4% of the respondents are critical or rather critical of surveillance (N=613).

Critique of Surveillance 1: If you have nothing illegal to hide, then you need not be afraid of surveillance.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Completely disagree	218	32,3	35,6	35,6
	Disagree	138	20,5	22,5	58,1
	Disagree somewhat	84	12,5	13,7	71,8
	Agree somewhat	84	12,5	13,7	85,5
	Agree	61	9,1	10,0	95,4
	Strongly agree	28	4,2	4,6	100,0
	Total	613	90,9	100,0	
Missing	System	61	9,1		
Total		674	100,0		

Table 7. Critical standpoints towards surveillance #1

Critique of Surveillance 2: I trust that social networking platforms such as studiVZ, MySpace, or Facebook deal in a responsible way with my data.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Completely disagree	74	11,0	12,1	12,1
	Disagree	137	20,3	22,3	34,4
	Disagree somewhat	114	16,9	18,6	53,0
	Agree somewhat	132	19,6	21,5	74,6
	Agree	112	16,6	18,3	92,8
	Strongly agree	44	6,5	7,2	100,0
	Total	613	90,9	100,0	
Missing	System	61	9,1		
Total		674	100,0		

Table 8. Critical standpoints towards surveillance #2

Critique of Surveillance 3: In Austria, there are only few laws that allow the surveillance of Internet and phone communication. Citizens are therefore well protected from state surveillance.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Completely disagree	79	11,7	12,9	12,9
	Disagree	159	23,6	25,9	38,8
	Disagree somewhat	211	31,3	34,4	73,2
	Agree somewhat	116	17,2	18,9	92,2
	Agree	42	6,2	6,9	99,0
	Strongly agree	6	0,9	1,0	100,0
	Total	613	90,9	100,0	
Missing	System	61	9,1		
	Total	674	100,0		

Table 9. Critical standpoints towards surveillance #3

Critique of Surveillance 4: Firms have a strong interest in gathering personal data of Internet users.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Completely disagree	14	2,1	2,3	2,3
	Disagree	8	1,2	1,3	3,6
	Disagree somewhat	18	2,7	2,9	6,5
	Agree somewhat	40	5,9	6,5	13,1
	Agree	145	21,5	23,7	36,7
	Strongly agree	388	57,6	63,3	100,0
	Total	613	90,9	100,0	
Missing	System	61	9,1		
	Total	674	100,0		

Table 10. Critical standpoints towards surveillance #4

Critique of Surveillance 5: State surveillance of citizens has increased after the terrorist attacks in New York on September 11, 2001.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Completely disagree	15	2,2	2,4	2,4
	Disagree	22	3,3	3,6	6,0
	Disagree somewhat	59	8,8	9,6	15,7
	Agree somewhat	156	23,1	25,4	41,1
	Agree	190	28,2	31,0	72,1
	Strongly agree	171	25,4	27,9	100,0
	Total	613	90,9	100,0	
Missing	System	61	9,1		
	Total	674	100,0		

Table 11. Critical standpoints towards surveillance #5

Critique of Surveillance Index
N=613 (Index=0 (uncritical of surveillance society) missing in figure because 0% of respondents belong to this category)

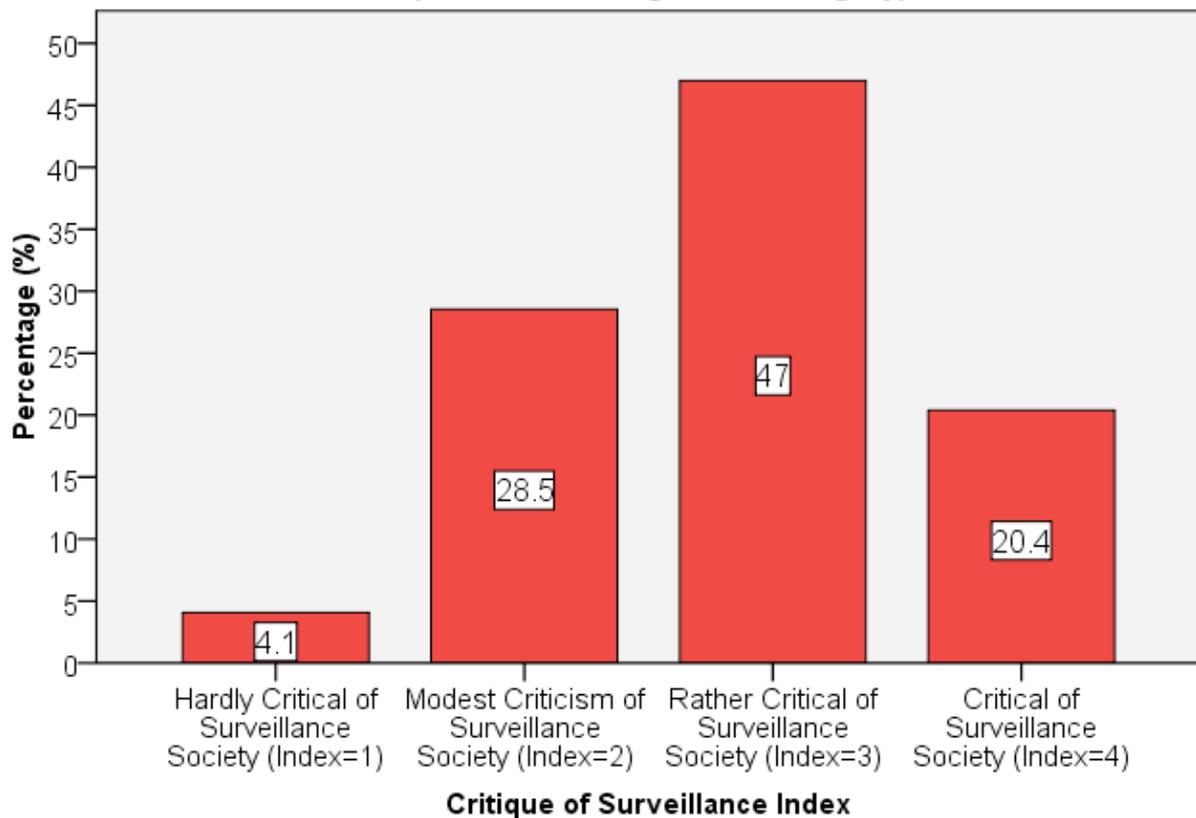


Figure 16. Surveillance critique index

Table 12 shows bivariate correlations between the surveillance critique index and other factors. The result is that the surveillance critique index is significantly (at the 0.01 level) negatively correlated to female gender (positively to male gender), studying natural sciences, and the usage frequency of ISNS. It is significantly (at the 0.01 level) positively correlated to the number of semesters studied, studying social sciences, and income. Being female decreases the probability of being critical of surveillance, whereas being male increases it. A reason for this influence could be patriarchal societal structures that construct women as being irrational and incapable of using and understanding technology. It can be an outcome of these structures that women show less interest in technology and the influence of technology on society than men. Surveillance is a topic that is strongly connected to data collection and electronic data processing. Studying natural sciences decreases the likelihood of being critical of surveillance, whereas studying social sciences increases this likelihood. Natural scientists tend to learn positivistic research methods and are interested in nature, whereas social scientists also employ more qualitative methods and are more frequently confronted with critical theories and critical research in their studies than natural scientists. Positivism is only interested in how something is, whereas critical thinking is interested in suppressed potentials and in what something could become and how it can be improved. Positivism is instrumental, whereas criticism is non-instrumental (Horkheimer 1947/1995).

“Modern science, as positivists understand it, refers essentially to statements about facts, and therefore presupposes the reification of life in general and of perception in particular. It looks upon the world as a world of facts and things, and fails to connect the transformation of the world into facts and things with the social process. The very concept of ‘fact’ is a product – a product of social alienation; in it, the abstract object of exchange is conceived as a model for all objects of experience in the given category. The task of critical reflection is not merely to understand the various facts in their historical development – and even this has immeasurably wider implications than positivist scholasticism has ever dreamed of – but also to see through the notion of fact itself, in its development and therefore in its relativity. The so-called facts that the positivists are inclined to regard as the only scientific ones, are often surface phenomena that obscure rather than disclose the underlying reality” (Horkheimer 1974/2004: 56).

Students who use ISNS frequently are more likely to be rather uncritical of surveillance. Surveillance is invisible. Foucault as a central characteristic of disciplinary surveillance power already characterized the principle of “seeing without being seen”.

“The Panopticon is a machine for dissociating the see/being seen dyad: in the peripheric ring, one is totally seen, without ever seeing; in the central tower, one sees everything without ever being seen” (Foucault 1977: 201f).

If one uses information and communication technologies frequently and does not see any immediate evidence of being under surveillance, then one might become more trusting in online platforms in particular and in the harmlessness of surveillance in general. Surveillance is a phenomenon that tries to naturalize and normalize itself, i.e. students, who have studied an upper number of semesters, are more likely to be critical of surveillance than other students. Graduate and doctoral students are more educated

than undergraduate students. This higher degree of education might enable a certain share of them to develop more critical outlooks on the world, including the topic of surveillance, than undergraduate students. Students with higher incomes are more likely to be critical of surveillance. An explanation for this influence can be that higher incomes allow students to access more and more diverse information sources and cultural sources, which increases the likelihood that they are confronted with critiques of surveillance.

In our study, gender, the type and extension of higher education, class, and usage frequency of social networking sites are factors that influence the degree of critical consciousness on surveillance.

	Surveillance Critique Index
Female: Correlation Coefficient Sig. (2-tailed) N	-0.200** 0.000 548
Male: Correlation Coefficient Sig. (2-tailed) N	0.200** 0.000 548
Age: Correlation Coefficient Sig. (2-tailed) N	0.169 0.000 613
Undergraduate Student: Correlation Coefficient Sig. (2-tailed) N	-0.078 0.055 613
Graduate Student: Correlation Coefficient Sig. (2-tailed) N	-0.031 0.440 613
Doctoral Student: Correlation Coefficient Sig. (2-tailed) N	0.095 0.019 613
Semesters: Correlation Coefficient Sig. (2-tailed) N	0.120** 0.003 601
Social Sciences, Humanities: Correlation Coefficient Sig. (2-tailed) N	0.196** 0.000 601
Natural Sciences: Correlation Coefficient Sig. (2-tailed) N	-0.127** 0.002 601
Engineering Sciences: Correlation Coefficient Sig. (2-tailed) N	-0.019 0.640 601
Fine Arts: Correlation Coefficient	-0.087

Sig. (2-tailed) N	0.033 601
Sports: Correlation Coefficient Sig. (2-tailed) N	-0.011 0.782 601
Medical Science: Correlation Coefficient Sig. (2-tailed) N	0.013 0.743 601
Law: Correlation Coefficient Sig. (2-tailed) N	-0.098 0.017 601
Income: Correlation Coefficient Sig. (2-tailed) N	0.115** 0.005 610
Size of Dominant Location: Correlation Coefficient Sig. (2-tailed) N	0.048 0.233 613
Highest Educational Achievement of Parents: Correlation Coefficient Sig. (2-tailed) N	-0.006 0.883 613
Father Blue Collar Worker: Correlation Coefficient Sig. (2-tailed) N	-0.048 0.236 613
Father White Collar Worker: Correlation Coefficient Sig. (2-tailed) N	0.005 0.905 613
Father Civil Servant: Correlation Coefficient Sig. (2-tailed) N	0.029 0.478 613
Father Self-Employed: Correlation Coefficient Sig. (2-tailed) N	-0.015 0.710 613
Father Retiree: Correlation Coefficient Sig. (2-tailed) N	0.006 0.885 613
Father Unemployed: Correlation Coefficient Sig. (2-tailed) N	0.079 0.050 613
Father Househusband: Correlation Coefficient Sig. (2-tailed) N	0.009 0.826 613
Mother Blue Collar Worker: Correlation Coefficient Sig. (2-tailed)	0.020 0.618

N	613
Mother White Collar Worker: Correlation Coefficient Sig. (2-tailed) N	0.003 0.932 613
Mother Civil Servant: Correlation Coefficient Sig. (2-tailed) N	0.064 0.114 613
Mother Self-Employed: Correlation Coefficient Sig. (2-tailed) N	0.033 0.416 613
Mother Retiree: Correlation Coefficient Sig. (2-tailed) N	-0.048 0.239 613
Mother Unemployed: Correlation Coefficient Sig. (2-tailed) N	-0.018 0.654 613
Mother Housewife: Correlation Coefficient Sig. (2-tailed) N	-0.080 0.048 613
Usage Intensity ISNS: Correlation Coefficient Sig. (2-tailed) N	-0.172** 0.000 613
Read Terms of Use: Correlation Coefficient Sig. (2-tailed) N	0.083 0.041 613
** Correlation is significant at the 0.01 level (2-tailed)	

Table 12. Bivariate correlations of surveillance critique index and other factors

Our study shows that the knowledge about surveillance of students in Salzburg is rather low, whereas their critical attitude towards surveillance is rather high. The knowledge and the critique index are positively correlated: The more knowledge students have about surveillance, the more critical they tend to become. There is a positive correlation that is significant at the 0.01 level (see table 13). The more critical they are, the more knowledge they tend to have about surveillance. How can it be explained that there seems to be little knowledge of actual surveillance, but a high level of criticism towards surveillance? The students in our survey tend to see surveillance as a problem. So for example an overwhelming majority of them thinks that corporations have an interest in gathering and using data and says that one needs to be afraid of surveillance even if one has done nothing illegal and does not intend to break the law. There seems to be a general feeling of students that surveillance is dangerous, threatens the privacy of all individuals, and creates a climate, in which one is automatically considered to be a potential criminal or terrorist. So young people seem to be socialized in a way that tends to create suspicion towards surveillance. For example many pupils in school read and discuss books like George Orwell's "1984" and Aldous Huxley's "Brave New World". But there is not much knowledge about the actual laws in Europe and Austria

that regulate surveillance. So for example the amendment of §53 of the Austrian Security Police Act (Sicherheitspolizeigesetz) at the end of 2007 and the European Data Retention Directive are hardly known. Our interpretation is that Austrian institutions (such as the educational system, schools, universities, politicians and the political system, or the media) provide young people with the impression that surveillance as such is dangerous, but that it is not something one has to worry about in Austria. There seems to be a lack of information about concrete Austrian surveillance policies and a lack of problematization of surveillance by cultural and political institutions in Austria.

	Surveillance Critique Index
Surveillance Knowledge Index:	
Pearson Correlation	0.283**
Sig. (2-tailed)	0.000
N	613
** Correlation is significant at the 0.01 level (2-tailed).	

Table 13. Bivariate correlation between the surveillance knowledge index and the surveillance critique index

The Austrian Security Police Act was amended on December 6th, 2007. Data protectors argued that this amendment has given the police extended possibilities for surveillance (see for example a comment by Arge Daten²⁵). We conducted a search in the APA Defacto Archive of Austrian newspapers for finding out how many articles on the Austrian Security Police Act were published from November 22 until December 20, 2007 (the time from 2 weeks before and 2 weeks after the bill's amendment). Table 14 shows the results. From November 22 until December 20, 2007, a total of 23 articles that dealt primarily with the amendment of the security police act were published in 8 Austrian newspapers. Given the fact that there was harsh criticism of the Austrian Security Police Act (for example by the Austrian Green Party, Arge Daten, the League of Human Rights) and that the Green Party initiated a petition for the protection from the surveillance state, 23 articles within one month on a pressing topic can be considered a rather low number. Until the end of 2007, the police on average asked Internet Service Providers (ISP) for approximately 1000 user identifications per year²⁶. According to a parliamentary inquiry by the Austrian Green Party, there were 3863 user identification demands by the police to Internet and mobile phone providers from January to April 2008 based on the amended Security Police Act²⁷. These are on average 32 police surveillance inquiries per day and $365 \cdot 32 = 11\ 680$ inquiries per year.

²⁵ *Sicherheitspolizeigesetz: Noch weitere Eingriffe abgenickt*, Arge Daten, December 6, 2007, http://www2.argedaten.at/session/anonym283144otaspp709845.E42_INP.html, accessed on December 6, 2008

²⁶ *Internet: Tausende Illegal ausgeforscht*, Die Presse, November 9, 2008, <http://diepresse.com/home/techscience/internet/428919/index.do?from=suche.intern.portal>, accessed on December 7, 2008

²⁷ *Polizei überwacht täglich 32 Handy- und Internetnutzer*, Die Presse, June 25, 2008, <http://diepresse.com/home/techscience/hightech/mobil/393783/index.do?from=suche.intern.portal>, accessed on December 7, 2008. <http://www.ueberwachungsstaat.at/index.php?id=56263>, accessed on December 7, 2008.

Newspaper Title	Number of articles on the amendment of the Security Police Act (November 22-December 20, 2007, Source: APA DeFacto, www.defacto.at)	Audience Scope (% of population consuming a medium, Mediaanalyse 2007/2008, media-analyse.at)
Kronen Zeitung	0	42.2%
Kleine Zeitung	7	11.7%
Kurier	4	8.7%
Der Standard	3	5.0%
Oberösterreichische Nachrichten	1	4.8%
Die Presse	2	3.6%
Salzburger Nachrichten	1	3.6%
Vorarlberger Nachrichten	5	2.9%
Total	23	

Table 14. Number of articles on the amendment of the Security Police Act in selected Austrian newspapers (November 22-December 20, 2007; Source: APA DeFacto, search keyword: Sicherheitspolizeigesetz)

There was low media coverage on the amendment of the Austrian Security Police Act in December 2007. This is not an empirical prove, but an indication that there is not much media coverage and public problematization of surveillance in Austria. A lack of information and of public discussion could be one of the reasons why the students in our survey tend to be rather critical of surveillance, but tend to have little knowledge of the actual judicial situation of surveillance in Austria and Europe.

7.4. Usage of studiVZ

88.3% of our respondents are studiVZ users (figure 17). This confirms the fact that studiVZ is the most used ISNS in Austria and Germany. 91.8% of the studiVZ users answered correctly that studiVZ gathers and stores data about their usage behaviour (figure 18). 85.6% of the studiVZ users know that studiVZ does not reuse and resell personal data of users (figure 19). These two results show that students in Salzburg have a relatively good knowledge of what studiVZ is allowed and not allowed to do with their data. 46.6% of the studiVZ users have read the new terms of use that were introduced at the beginning of 2008, whereas 41.8% have not read them (figure 20). This is a relatively balanced distribution. For the majority of users (55.2%), trust into studiVZ has remained the same after the new terms of use took effect. For a small minority, trust has increased (6.1%), for 38.7% it has decreased (figure 21). 75.0% of the studiVZ users have deactivated to receive messages from studiVZ advertising clients per email or the studiVZ message service (figure 22). 58.04% have deactivated receiving personalized advertisements (figure 23). 69.1% have deactivated the option that studiVZ can send them announcements on new features (figure 24). Combining these three information behaviours by adding one point for each deactivation, we calculated the studiVZ information behaviour index (figure 25). 22.6% of the studiVZ users in our sample have no safety from advertisements, 7.8% low safety, 20.5% some safety, and 49.2% good safety.

These results show that students in Salzburg who use studiVZ tend to have good knowledge of what studiVZ is allowed to do with their data and tend to have taken steps for guaranteeing that advertising and personalized advertising are minimized.

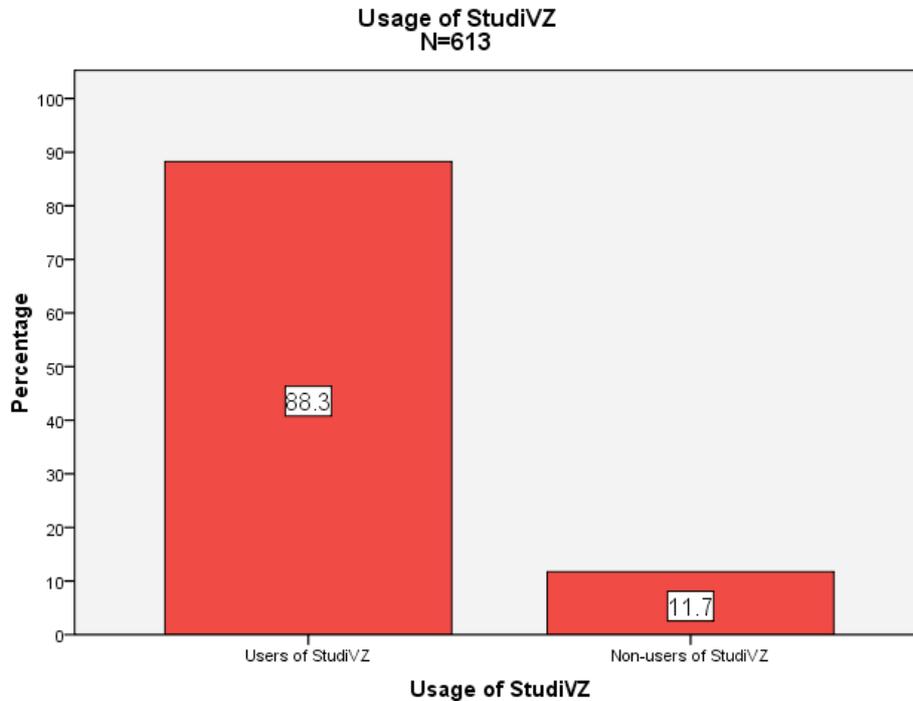


Figure 17. Share of studiVZ users

studiVZ knowledge #1: studiVZ gathers and stores data on my usage behaviour on the platform (visited pages, time of log in, sending of messages and entries, membership in groups, etc). N=401

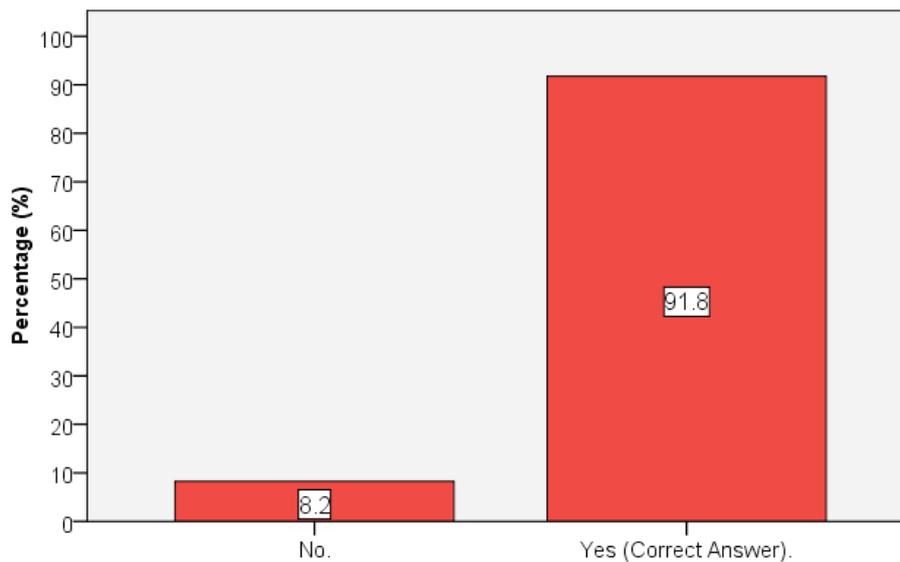


Figure 18. Knowledge about studiVZ #1

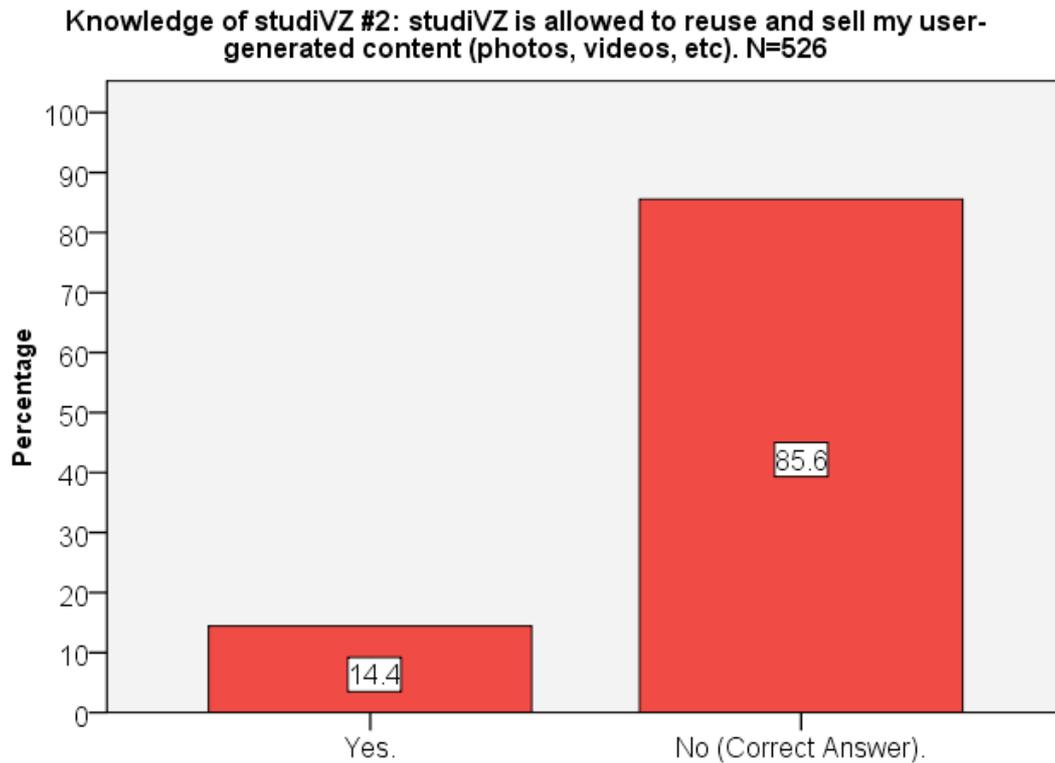


Figure 19. Knowledge about studiVZ #2

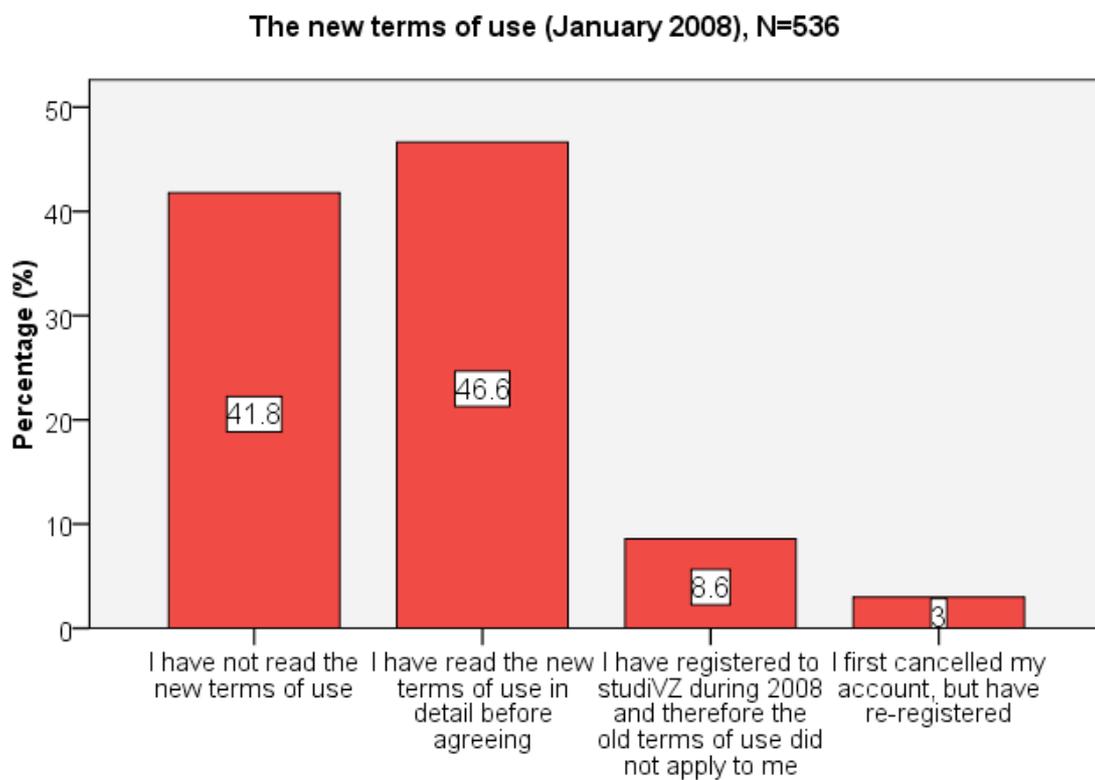


Figure 20. Behaviour concerning the new terms of use of studiVZ

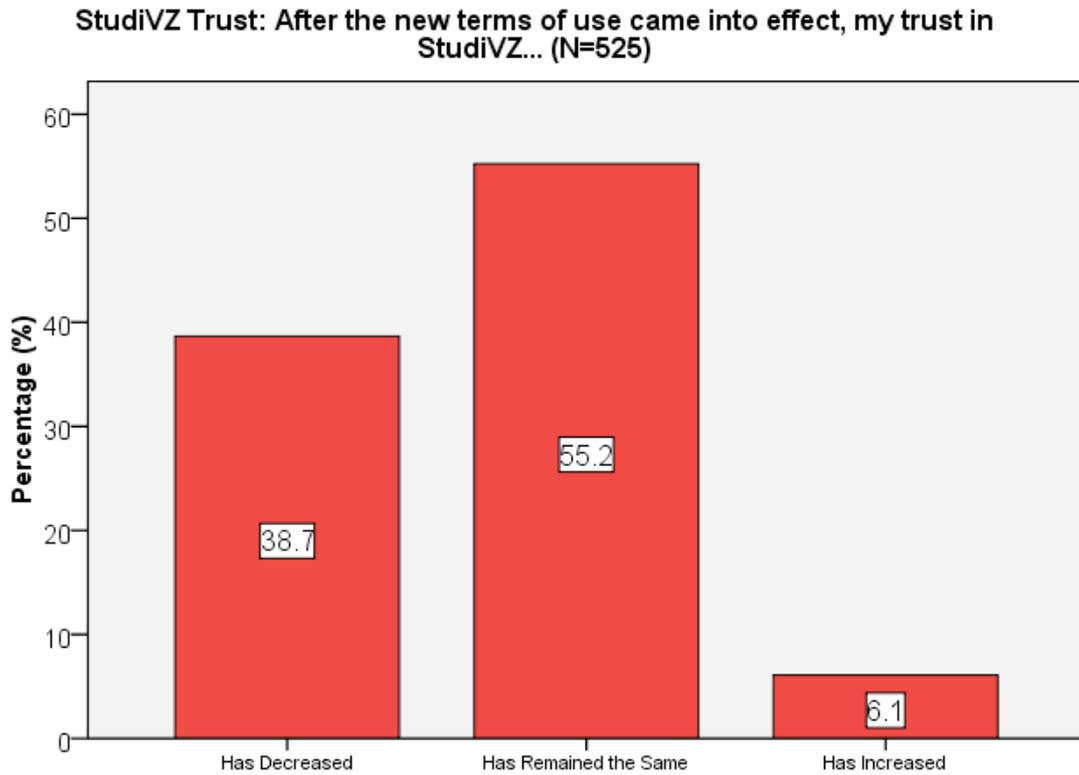


Figure 21. Trust in studiVZ

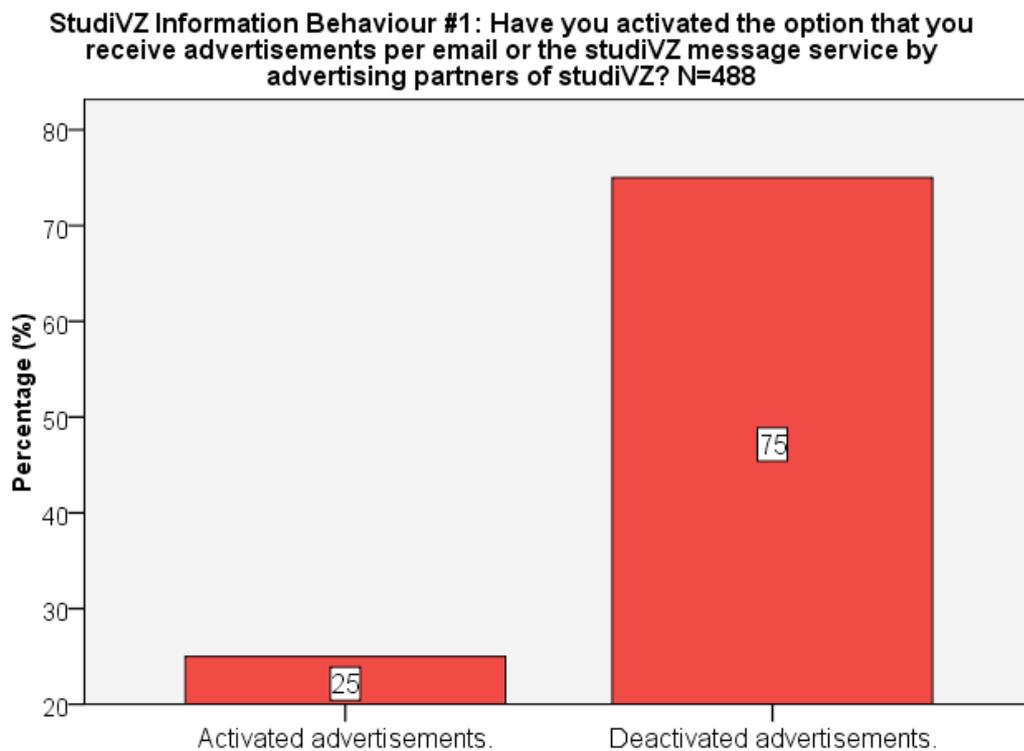


Figure 22. studiVZ information behaviour #1

StudiVZ Information Behaviour #2: Personalized advertisement, N=488

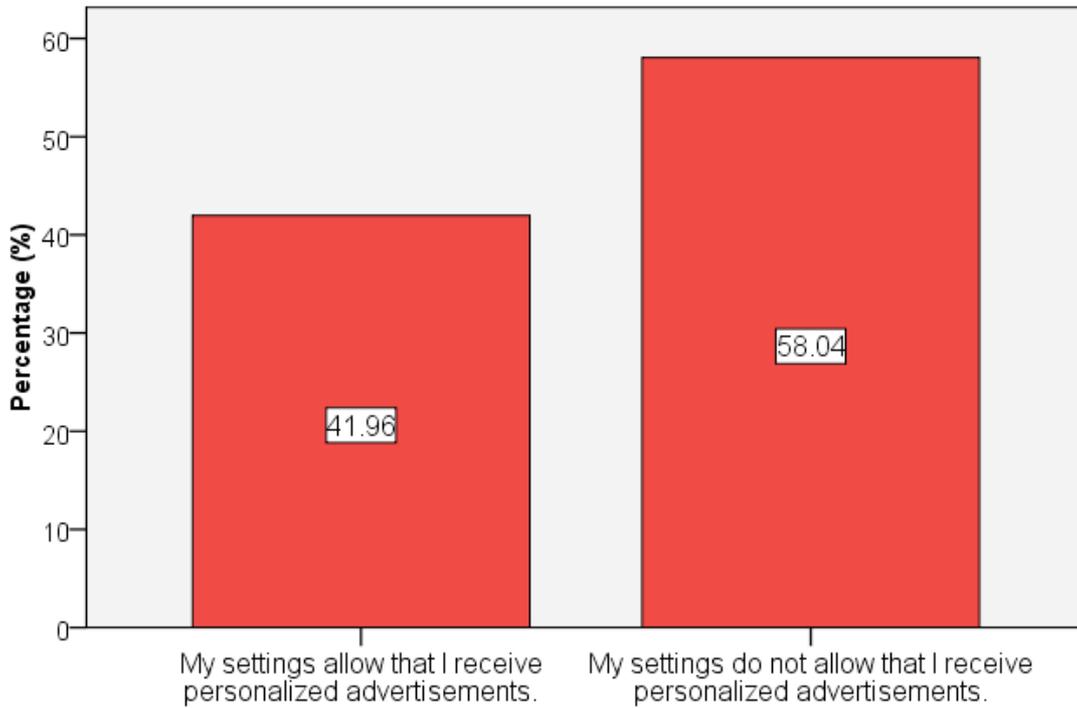


Figure 23. studiVZ information behaviour #2

StudiVZ Information Behaviour #3: I have selected the option that studiVZ can send me information about new features, events, or special offers per email or the studiVZ message service, N=511

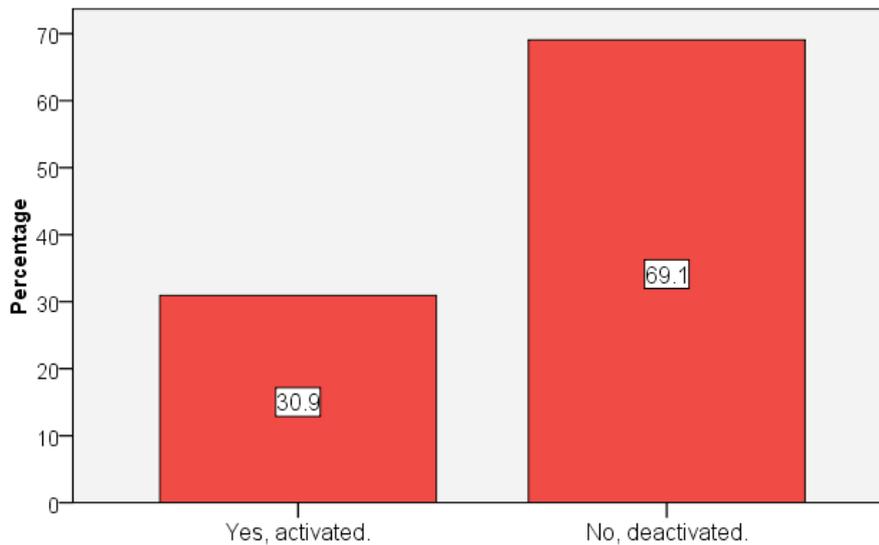


Figure 24. studiVZ information behaviour #3

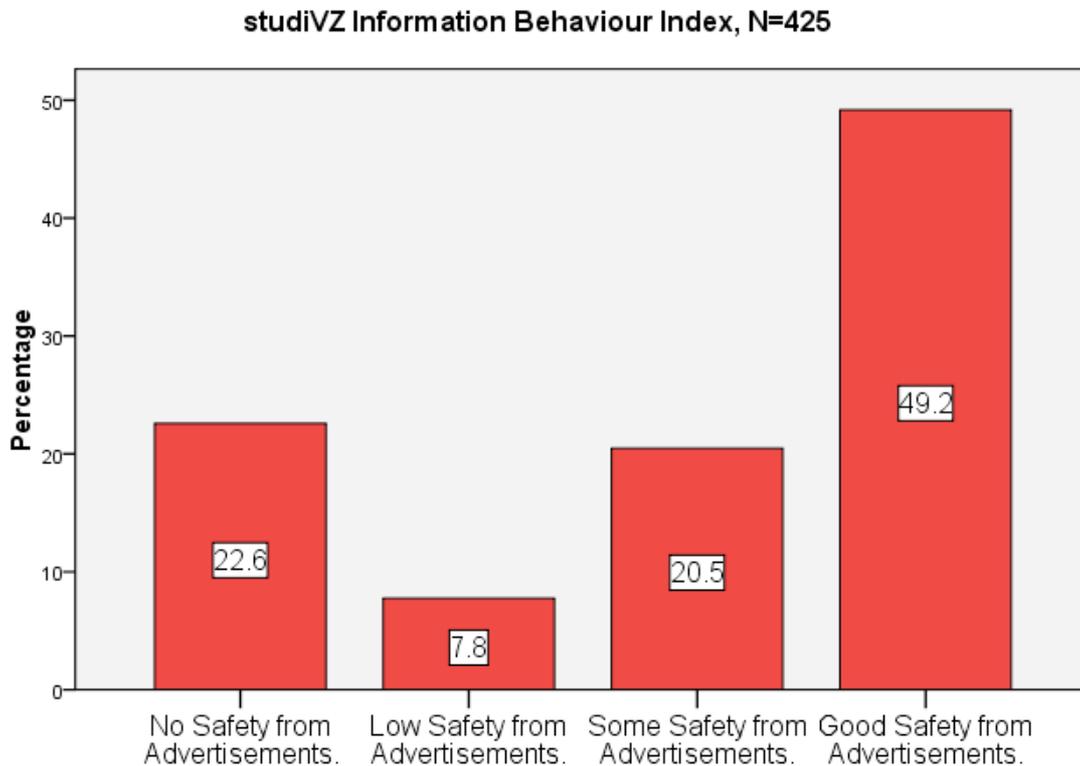


Figure 25. studiVZ information behaviour index

Table 15 presents the results of bivariate correlations between those variables that concern studiVZ on the one hand (knowledge about studiVZ, if users have read the new terms of use before accepting them, how their trust in studiVZ has changed after the new terms of use took effect, and the studiVZ information behaviour index) and certain factors on the other hand (usage intensity of SNS, intensity of reading terms of use in general, surveillance critique index, surveillance knowledge index). The results show that the knowledge users have about what studiVZ is allowed to do with their personal data is positively correlated with the surveillance critique index at a significance level of 0.01. This means that being critical of surveillance increases the probability that users inform themselves on what studiVZ is allowed to do. Users who read the terms of use of ISNS in general in more detail tend to have read the new terms of use of studiVZ. This is an obvious result. That there is a significant correlation (at the 0.01 significance level) between those two aspects is a confirmation that the survey respondents have given correct answers. The trust of users in studiVZ tends to have decreased after the new terms of use took effect, if these users have read the new terms, read terms of use in general, are critical of surveillance, and have knowledge of surveillance. The intensity of reading terms of use and the surveillance critique index are positively correlated with the studiVZ information behaviour index at the 0.01 significance level. This means that users tend to deactivate the possibilities that studiVZ has for sending them advertisings or personalized advertisings, if they tend to read terms of use in general and if they are critical of surveillance.

	studiVZ Knowledge #1	studiVZ Knowledge #2	Having Read the New Terms of Use	Trust in studiVZ	studiVZ Information Behaviour Index
Having Read the New Terms of Use: Correlation Coefficient Sig. (2-tailed) N				-0.182** 0.000 386	
Usage Intensity ISNS: Correlation Coefficient Sig. (2-tailed) N	0.016 0.746 401	0.112** 0.010 526	0.055 0.272 396	0.082 0.059 525	0.050 0.304 425
Read Terms of Use: Correlation Coefficient Sig. (2-tailed) N	0.030 0.552 401	0.069 0.114 526	0.358** 0.000 396	-0.181** 0.000 525	0.165** 0.001 425
Surveillance Critique Index: Correlation Coefficient Sig. (2-tailed) N	0.137** 0.006 401	0.139** 0.001 526	0.093 0.064 396	-0.270** 0.000 525	0.157** 0.001 425
Surveillance Knowledge Index: Correlation Coefficient Sig. (2-tailed) N	0.081 0.104 401	-0.096 0.028 526	0.092 0.068 396	-0.159** 0.000 525	0.089 0.066 425
** Correlation is significant at the 0.01 level (2-tailed).					

Table 15. Bivariate correlations about studiVZ

Although students tend to rather not read terms of use and privacy policies of social networking sites in general (12.9% say they never read them never, 36.6% say they read them only superficially, whereas only 11.7% say they read them almost entirely and 2.2% that they read them always in detail), in the case of the new terms of use of studiVZ that were introduced at the beginning of 2008, 46.6% of the studiVZ users said that they had read the terms in detail before agreeing and 38.7% say that their trust in studiVZ decreased after the new terms had come into effect. This is an indication that studiVZ users were suspicious why new terms were introduced and that they heard about increased possibilities for economic surveillance and privacy threats that the new terms of use could bring about. Public discussion about the new terms of use and its problems could be one of the factors that influenced the information behaviour of studiVZ users.

The studiVZ users in our survey are highly knowledgeable of what studiVZ is allowed to do and is not allowed to do with their personal data. 91.8% of them know that studiVZ gathers and stores data on their usage behaviour, 85.6% answer correctly that studiVZ is not allowed to reuse or resell user-generated content. This is an indication that the users are well informed about the terms of use and the rights that studiVZ has reserved for itself legally. Public discourse could be one of the factors that influenced this high degree of knowledge about studiVZ. After the new terms of use had come into effect, the standard advertising settings for all old and new users were that advertising clients

of studiVZ are allowed to send ads to users per email and the studiVZ message service, that personalized advertising is enabled, and that studiVZ can send announcements to users. 75.0% of the studiVZ users in our sample have actively opted out of the first advertising option, 58.04% have opted out of the second advertising option, and 69.1% have opted out of the third advertising option. In total, 49.2% have opted out of all three advertising options and 20.5% have opted out of two advertising options. 7.8% have opted out from only one advertising option and 22.6% have not opted out of any advertising option. These data show that 70% of all studiVZ users in our sample have a critical behaviour towards advertising. They are informed about which advertising options studiVZ has introduced and want to limit the amount of advertising they receive. The degree of critique towards surveillance in general influences the knowledge about studiVZ and critical information behaviour. The more critical the users are about surveillance in general, the more they tend to know about what studiVZ does with their data and the more they tend to deactivate advertising options.

We can conclude from these data that there is a positive relationship between the level of critique of surveillance on the one hand and on the other hand knowledge about studiVZ and critical information behaviour on the studiVZ platform. Information about the changes in privacy, surveillance, and advertising that studiVZ planned by introducing new terms of use, seems to have activated the critical potential of the students that is present in the form of a general critical attitude towards surveillance so that a majority of students have actively taken steps to limit the amount and type of advertising they receive. There seems to be a general critical attitude of students towards advertising and the usage of personal data and user behaviour by third-party advertising clients.

The most read newspapers in Germany are Bild, Süddeutsche Zeitung, and Frankfurter Allgemeine Zeitung (Media Analyse Deutschland 2008, Tageszeitungen). The most read weekly magazines are Spiegel and Stern (Media Analyse Deutschland 2008, Zeitschriften). The change of the terms of use was a topic in the German press. In December 2008, Bild Zeitung presented ten digital flops of the year 2007. studiVZ was listed at rank number 4, arguing that studiVZ has introduced “new dubious terms of use”, based on which “user data will be assessed and used for personalized advertisement and ads per email and mobile phone. Furthermore data shall be passed on to public authorities”²⁸. Süddeutsche Zeitung featured an article on the change of the terms of use and its implications on December 15, 2007²⁹. Frankfurter Allgemeine

²⁸ *Die digitalen Tops und Flops 2007 [Digital Tops and Flops 2007]*, Bild, <http://www.bild.de/BILD/digital/technikwelt/2007/12/tops-flops/highlights-2007.html>,

accessed on December 7, 2008: “Das Studentenportal hat neue fragwürdige Geschäftsbedingungen angekündigt. Es sollen in Zukunft Nutzerdaten ausgewertet und für personalisierte Werbung per E-Mail und Handy verwendet werden. Außerdem sollen Daten an Behörden weitergegeben werden. Wer den AGB nicht zustimmt, wird automatisch aus dem sozialen Studentennetzwerk entfernt” [“The student portal has announced new dubious terms of use. In the future, user data will assessed and used for personalized advertising and ads per email and mobile phone. Furthermore data shall be passed on to public authorities. People who do not agree to the terms of use, are automatically deleted from the student social network”].

²⁹ *StudiVZ rudert zurück [StudiVZ Paddels Back]*, Süddeutsche Zeitung, December 15, 2007: “Nachdem bekannt geworden war, dass das Internetportal User-Daten gezielt für Werbung nutzen will, brach ein Sturm der Entrüstung los. Jetzt bemühen sich die StudiVZ-Betreiber darum, die Mitglieder zu besänftigen” [After it has become public that the Internet portal wants to use user data purposefully for advertising, a

Zeitung had an article on the issue on December 14, 2007³⁰. Stern presented an article on the topic on December 14, 2007³¹. Spiegel reported on December 18, 2007, and on January 14, 2008³².

In Austria, students are most likely to read quality newspapers on the one hand (because of their higher education status) and regional newspapers on the other hand (because they cover topics of immediate concern). Therefore we can assume that students in Salzburg are most likely to read Der Standard, Die Presse, and Salzburger Nachrichten. Der Standard reported on March 6 and March 18, 2008³³. Die Presse featured an article on surveillance on ISNS on January 22, 2008³⁴. Salzburger Nachrichten reported on December 14, 2007³⁵. Unihelp.cc is an information and discussion platform that many students in Salzburg use. On December 16, 2007,

storm of protest broke out. Now the studiVZ operators strive to be calm their members”].

³⁰ *StudiVZ nutzt Mitglieder-Daten für gezielte Werbung [StudiVZ Uses Member-Data for Targeted Advertising]*, Frankfurter Allgemeine Zeitung, December 14, 2007. “Der Weg in den Profit will die Studenten-Plattform StudiVZ mit der Einführung personalisierter Werbung finden” [The student platform StudiVZ wants to find the way into profitability with the the introduction of personalized advertising”].

³¹ *StudiVZ im Werbefieber [StudiVZ in Advertising Fever]*, Stern, December 14, 2007. “Erst hat der Holtzbrinck-Verlag Millionen investiert, jetzt will das Unternehmen mit dem StudiVZ verdienen. Personalisierte Werbung soll die Vorlieben der Nutzer ansprechen - ein Verkauf der Daten sei jedoch nicht vorgesehen” [“At first, Holtzbrinck publishing house invested millions, now the corporation wants to make profits with StudiVZ. Personalized advertising shall appeal to the preferences of the users – but selling the data is not envisaged”].

³² *Studenten demonstrieren gegen das SchnüffelVZ [Students demonstrate against the SniffleVZ]*, Der Spiegel, December 18, 2007. “Mitglieder des StudiVZ grämen sich wegen neuer Werbeformen: Obwohl der Betreiber seine AGB-Änderung zur Werbe-Personalisierung entschärft hat, gehen Studenten auf die Barrikaden. Sie säubern ihre Profile, löschen Fotos und schreiben krieglerische Parolen auf ihre Pinnwände” [“Members of StudiVZ worry about new kinds of advertising: Although the provider has defanged the terms of use in the case of personalized advertising, students storm the barricades. They clean their profiles, delete images, and write war paroles on their pinboards”].

Schonungslose Messbarkeit [Ruthless Measurability], Der Spiegel, January 14, 2008. “Der Druck der Investoren auf die Online-Gemeinschaften wächst. Mit gezielten Werbebotschaften sollen endlich Gewinne gemacht werden!” [“The pressure of investors on online community grows. With the help of targeted advertising, finally profits should be made”].

³³ “Kifferbilder” bei StudiVZ: Unternehmen darf Daten nun an Behörden herausgeben [“Pothead Images” on StudiVZ: Corporation is now allowed to Give Data to Authorities], Der Standard, March 6, 2008. “Nutzungsbedingungen ermöglichen ‘bessere Zusammenarbeit’ mit den Behörden” [“Terms of use enable ‘better co-operation’ with public authorities”].

Werbeoffensive soll StudiVZ in die Schwarzen Zahlen hieven [Advertising Offensive Shall Hoist StudiVZ into the Black], Der Standard, March 18, 2008. “Studentenportal will jetzt die fünf Millionen Mitglieder zu Geld machen - Werbung nach Zielgruppen, aber ohne Weitergabe der Daten” [“Student portal now wants to make money of its five million members – advertising based on target groups, but no data transfer”].

³⁴ *Soziale Netzwerke haben “mehr Information als die Stasi” [Social Networks Have “More Information than Stasi”]*, Die Presse, January 22, 2008. “Medien-Experte Speck erforscht soziale Netzwerke und warnt ihre Mitglieder vor bedenkenlosem ‘digitalen Exhibitionismus’” [“Media expert Speck researches social networks and warns their members of unconsidered ‘digital exhibitionism’”].

³⁵ *studiVZ macht personalisierte Werbung [studiVZ Conducts Personalized Advertising]*, Salzburger Nachrichten, December 14, 2007. “Das Online-Netzwerk studiVZ will aus seinem großen Nutzerstamm Profit schlagen: Die rund vier Millionen Mitglieder sollen künftig mit personalisierter Werbung angesprochen werden, die auf Alter, Geschlecht, Wohn- und Studienort sowie Studienfach zugeschnitten” [The online network studiVZ wants to make profit of its large stock of users: Ist approximately four million members shall in the future be addressed with personalized advertising that is targeted on age, gender, place of residence, place of study, and field of study”].

Unihelp reported: “Attention! studiVZ Markets Personal Data!!!”[“Achtung: studiVZ vermarktet persönliche Daten!!!“]. Five people commented. This is an unusual high number of comments because normally most of the articles have none or just one comment. This shows that the change of the terms of use is a topic that concerns students immediately.

If one compares these articles, then it becomes clear that most of them straightforward announced that the change of the terms of use means more surveillance and less privacy in order to maximize economic profits of the Holtzbrinck corporation.

Students are likely to read such articles in newspapers, magazines, and online because studiVZ is used by the vast majority of them and they therefore have an immediate interest in the topic. This coverage might have positively influenced their knowledge about studiVZ and the resulting information behaviour. But besides news coverage on the new studiVZ terms of use, there was also an online campaign, which was likely to attract many studiVZ users. On December 7, 2008, there were 248 interest and discussion groups on studiVZ that covered the issue of the new terms of use (Allgemeine Geschäftsbedingungen, AGB). Table 16 shows the five groups that had the most members.

Group Name	Number of Members	Number of Postings
Achtung - studiVZ ändert die AGB! [Attention – studiVZ changes the terms of use!]	3820	8748
Widerspruch gegen die neuen AGB (12/07) [Opposition to the new terms of use (12/07)]	1620	1042
"Stell dir vor, studiVZ ändert die AGB und keiner stimmt zu" ["Imagine that studiVZ changes the terms of use, but nobody agrees"]	875	201
Stell dir vor, studiVZ ändert die AGB und keiner stimmt zu 2 [Imagine that studiVZ changes the terms of use, but nobody agrees 2]	511	411
! Datenklau abstellen ! Vorgehen gegen Datenschutzerklärung/AGB! [! Stop data theft ! Action against privacy policy/terms of use!]	366	23

Table 16. studiVZ interest groups on the change of the terms of use with most members (accessed on December 7, 2008)

In the largest group, information about the changes are provided and there is an appeal that users should not agree (“Appeal to all members: Let your profiles become orphans!”, “Appell an alle Mitglieder: Lasst eure Profile verwaisen!”). It also documents links to press articles that cover the topic. All of these five groups argue that becoming a member of them is an expression of protest and that the users possess a collective power to leave studiVZ. The third group lists how the advertising options can be deactivated. There were also intense discussions in these groups that focused on appeals to spread the word about the change of the terms of use and the protest groups to other users, on gathering group members in order to create the threat of mass-withdrawal from studiVZ, and on discussions about surveillance.

Networked digital technologies pose quick, cheap, efficient means for organizing protest. Information about protests can be distributed (Cognitive cyberprotest), protest can be communicated and resistance can be co-ordinated (Communicative

cyberprotest), and protest actions can besides in real space be organized as joint online actions (Co-operative cyberprotest) (Fuchs 2008: 277-289). Notions such as cyberprotest (Van de Donk/Loader/Nixon/Rucht 2004) and cyberactivism (McCaughy/Ayers 2003) have been coined for describing the organization of protest with the help of ICTs.

Online behaviour by studiVZ users in reaction to the planned change of the terms of use mainly operated on the cognitive (spreading the information) and communicative (discussing consequences and strategies) level, there were no co-operative endeavours such as setting up a petition against the new terms of use. A mass withdrawal from studiVZ would have been a form of electronic civil disobedience, but was unlikely because only some thousand users joined the groups, which is not a critical mass given the fact that studiVZ has several million users. Therefore it is not so clear if one can even speak of cyberprotest in this case or only of an online information campaign. One weakness of the campaign was that many different groups were created, which fragments the online public and does not create one overall platform of discussion and one impressive amount of users that can engage in co-ordinated actions. A disadvantage of one overall group is that it is easier for the provider to shut down, keep under surveillance, and control protest. Distributed cyberprotest is harder to control, but tends to fragment the protest public, whereas united cyberprotest is easier to control, but creates a more powerful mass of activists.

Those users who were unsatisfied with the new terms did not succeed in circumventing the new terms of use. But the planned selling of user data to third parties was not included and is now explicitly barred in the new studiVZ terms of use. Our survey data indicate that the online information campaign succeeded in drawing attention to the issue of surveillance by studiVZ and led a vast majority of users to disable advertising options. Nonetheless personalized advertising and advertising messages per email and message service have been introduced and are now standard settings on studiVZ. The studiVZ information campaign did not attract a very large number of active users and seems not to have reached a co-operative level of protest, but it seems to have succeeded in bringing many users to deactivate advertising options. But of course advertising and targeted advertising continue to exist on studiVZ, which means that the platforms sells its users as an audience commodity to advertising clients in order to accumulate money capital.

Overall, media information and an online information campaign seem to be some of the causes of the high degree of knowledge and the high degree of critical information behaviour of the students in our sample in respect to studiVZ.

7.5. Usage of Facebook

39.5% of the respondents use Facebook (figure 26), which is clearly a lower number than in the case of Facebook (88.3%).

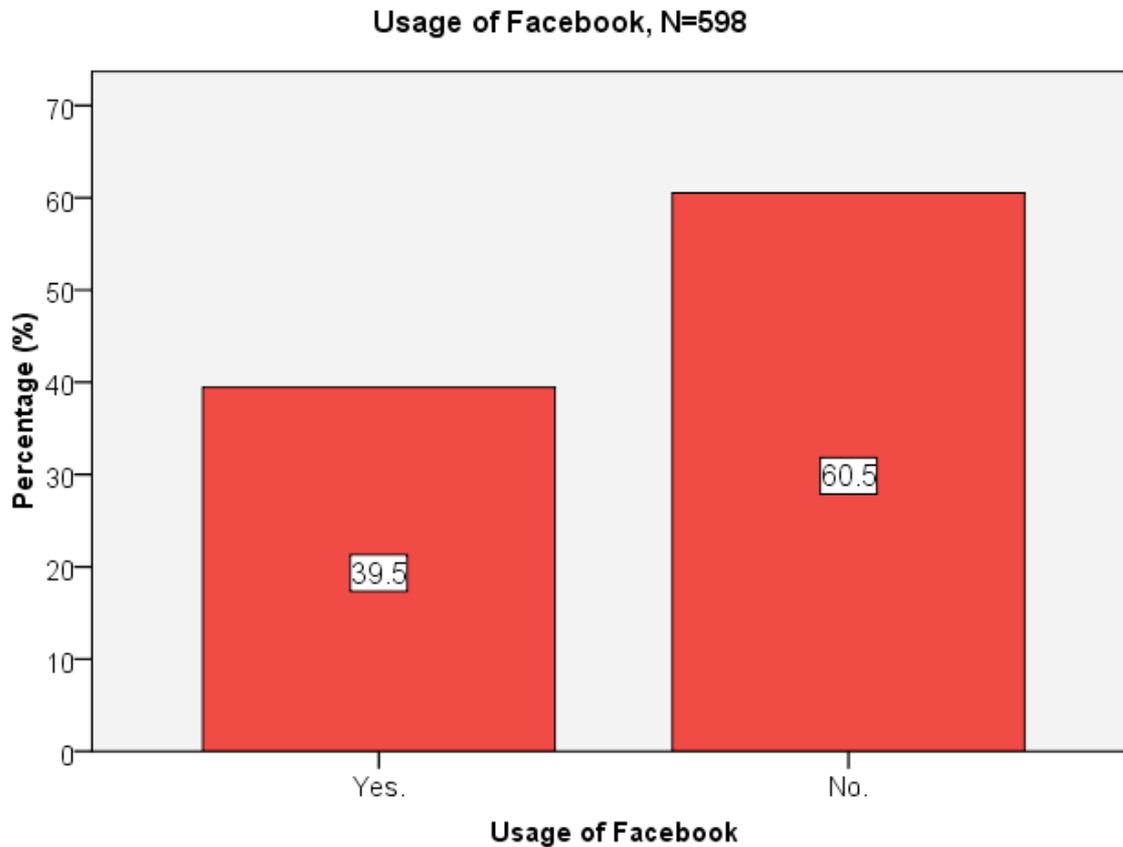


Figure 26. Usage intensity of Facebook

94.0% of the Facebook users in our survey answered correctly that Facebook is allowed to collect and store data on their information behaviour (figure 27). Only 20.4% knew that Facebook is allowed to reuse and resell personal data (figure 28). 54.5% knew that advertising clients of Facebook are allowed to gather data on the information behaviour of users (figure 29). Only 33.2% answered correctly that Facebook is always allowed to send them personalized advertising (figure 30). By combining the answers to these four questions, we calculated the Facebook knowledge index (figure 31): 4.7% of the Facebook users had little knowledge about Facebook (no correct answer), 31.5% small knowledge (one correct answer), 29.8% average knowledge (two correct answers), 26.0% good knowledge (three correct answers), and 8.1 a high degree of knowledge (four correct answers). This means that only 34.1% of the Facebook users had a good or high degree of knowledge about what Facebook is allowed to do with their data, whereas in the case of studiVZ users the degree of correct answers to such questions was on average 88.7% (=the average of 91.8% and 85.6%). The knowledge about what platforms are allowed to do with personal data is much higher in the case of studiVZ than in the case of Facebook. An explanation for this difference can be that studiVZ is more used, more discussed between friends, more discussed in the media, and had attracted the attention of many users when it changed its terms of use, whereas Facebook is less known and less discussed in personal conversations and in the public.

Knowledge of Facebook #1: Facebook is allowed to collect and store data on my information behaviour, N=235

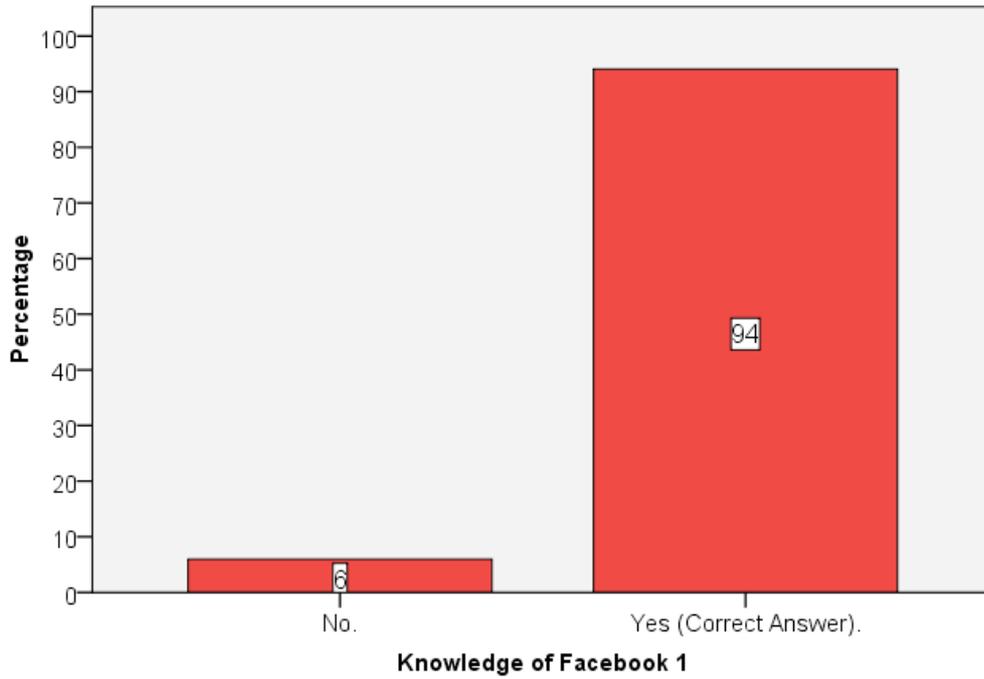


Figure 27. Knowledge about Facebook #1

Knowledge of Facebook #2: Facebook is allowed to reuse and resell my data, N=235

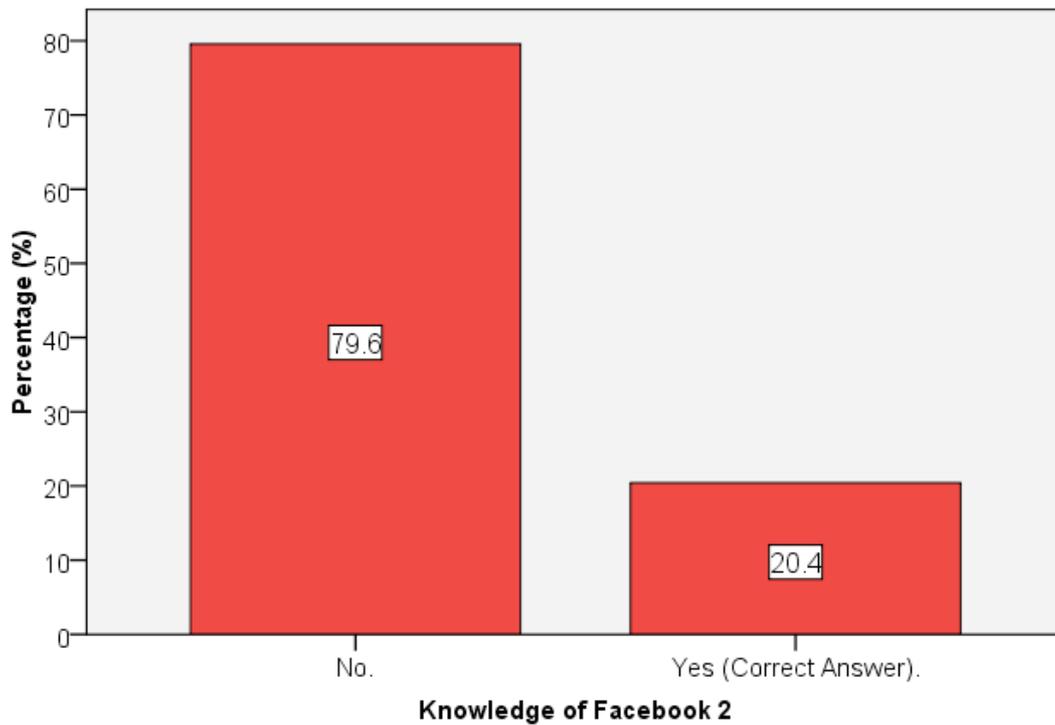


Figure 28. Knowledge about Facebook #2

Knowledge of Facebook #3: Advertising clients of Facebook are allowed to gather data on my information clients behaviour, N=235.

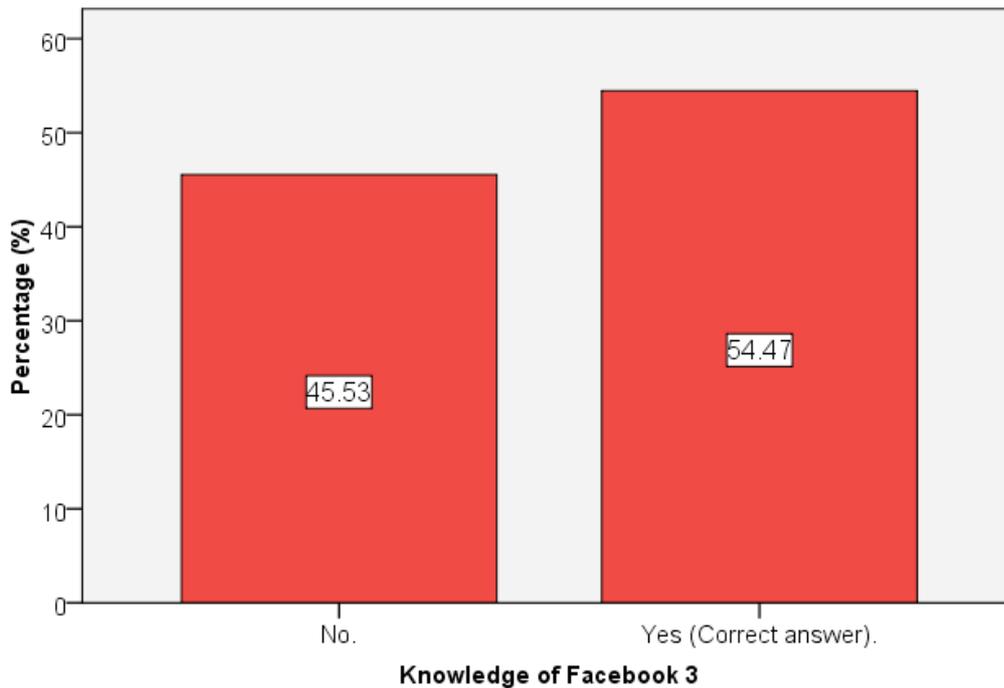


Figure 29. Knowledge about Facebook #3

Knowledge of Facebook #4: Facebook is allowed to send me personalized advertising, N=235

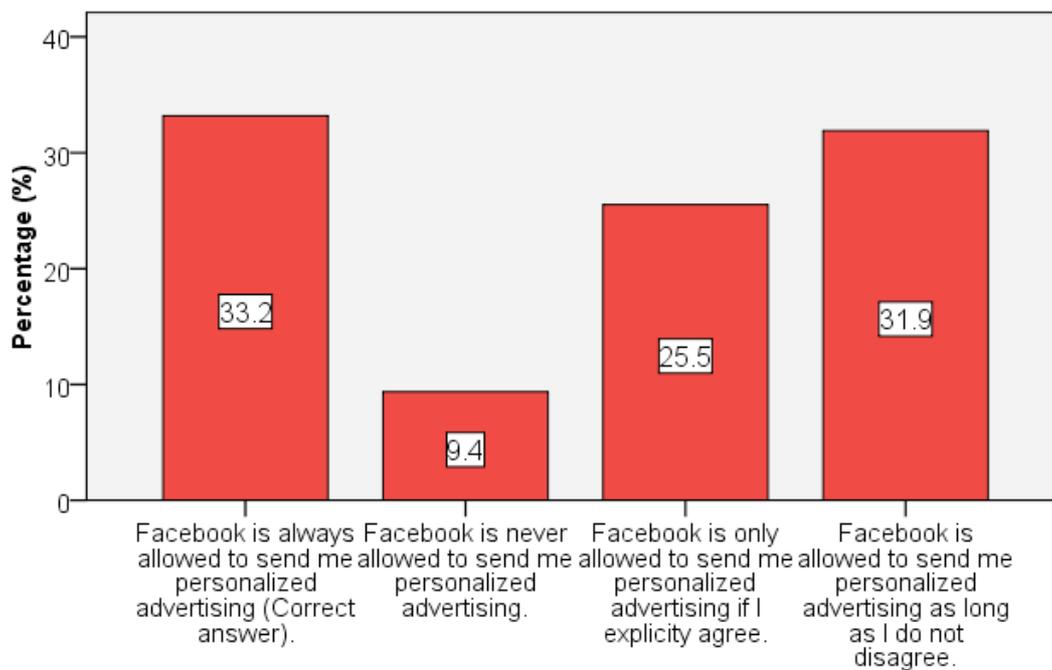


Figure 30. Knowledge about Facebook #4

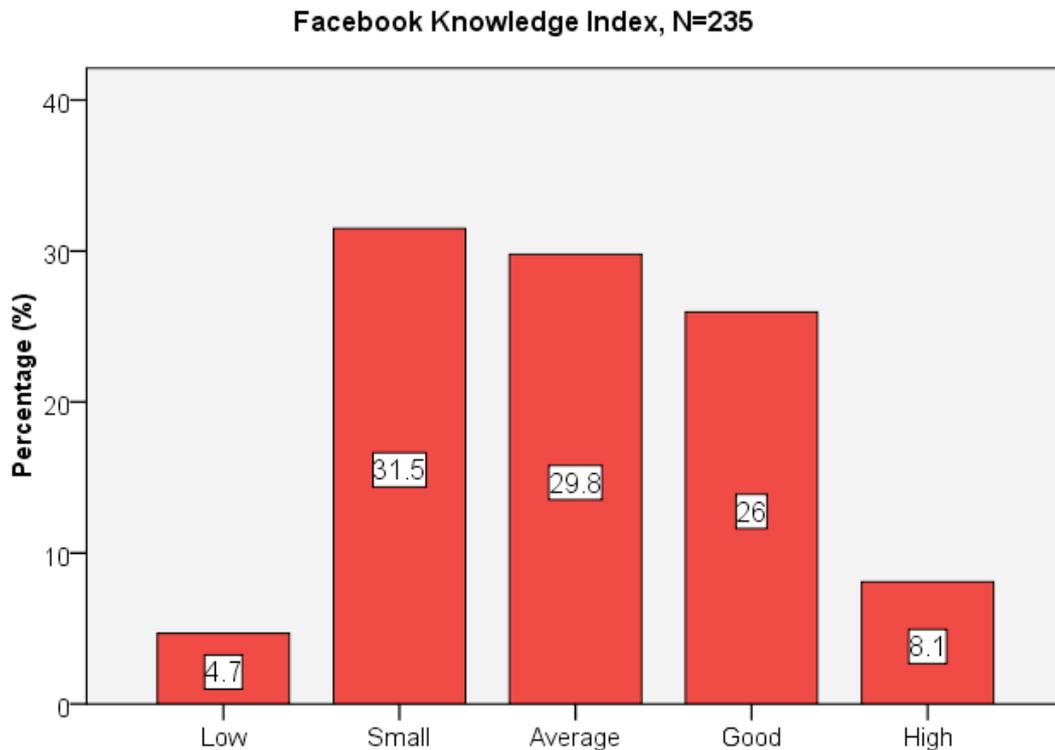


Figure 31. Facebook Knowledge Index

68.4% of the Facebook users in our survey have activated social advertisements on Facebook (social ads are a kind of personalized advertising that calculates ads based on friendship groups) (figure 32). 59.9% have activated Facebook beacon, which collects onsite and offsite usage data and publishes these on users' newsfeeds (figure 33). On studiVZ, on average 67.4% of the users in our survey have opted out of advertising options, whereas on Facebook on average only 35.9% of the users opted out of these options. This shows that critical information behaviour is higher on studiVZ than on Facebook. An explanation for this difference is that studiVZ is more known, more widely used, more discussed in personal conversations and in the public, and has attracted the attention of users and the public when it changed its terms of use.

Facebook Information Behaviour #1: Social Ads. N=206

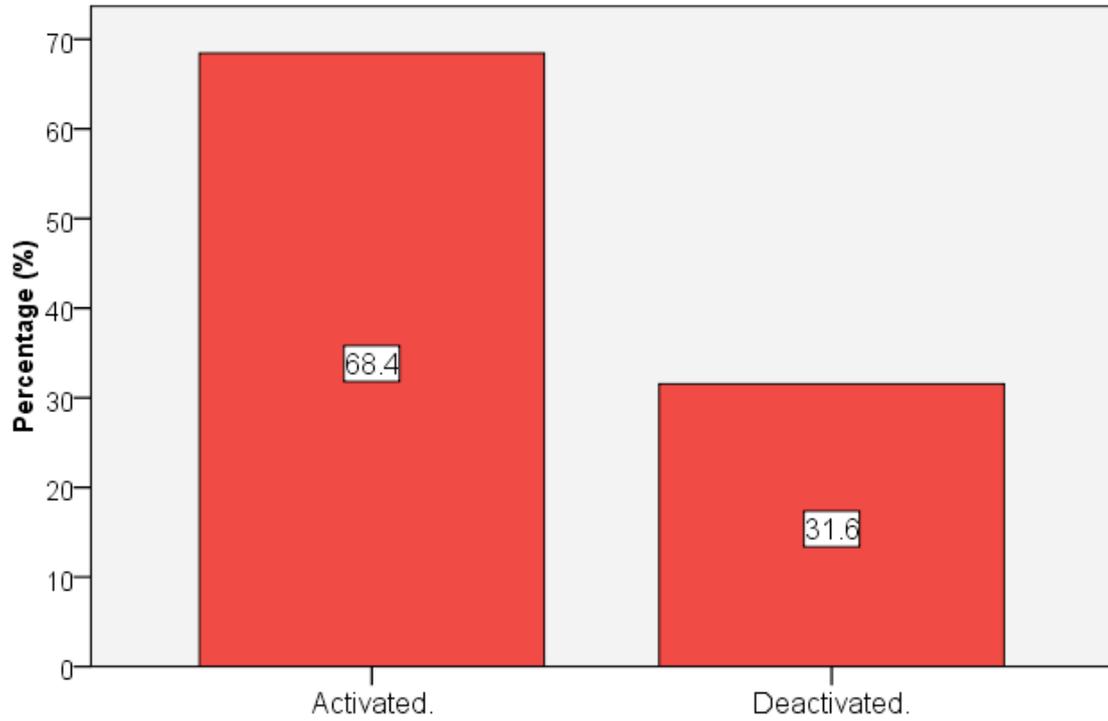


Figure 32. Facebook information behaviour #1

Facebook Information Behaviour #2: Facebook Beacon, N=227

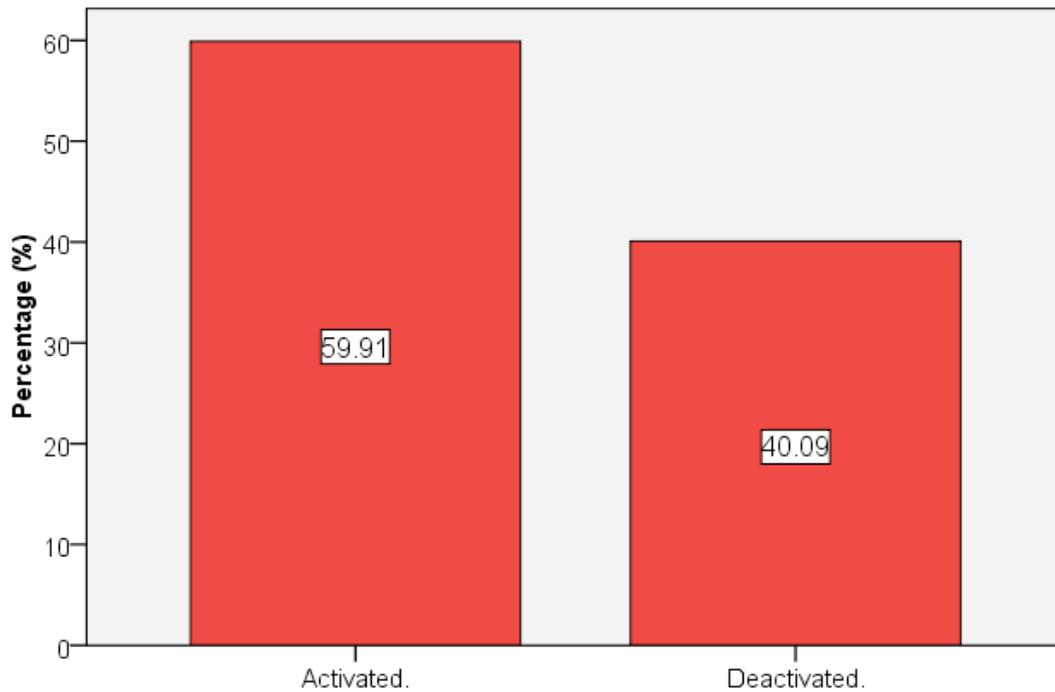


Figure 33. Facebook information behaviour #3

	Facebook Knowledge Index	Facebook Information Behaviour #1	Facebook Information Behaviour #2
Usage Intensity ISNS: Correlation Coefficient Sig. (2-tailed) N	-0.049 0.457 235	-0.049 0.487 206	-0.017 0.793 227
Read Terms of Use: Correlation Coefficient Sig. (2-tailed) N	0.008 0.908 235	0.144 0.040 206	0.126 0.058 227
Surveillance Critique Index: Correlation Coefficient Sig. (2-tailed) N	0.187** 0.004 235	0.008 0.909 206	-0.017 0.803 227
Surveillance Knowledge Index: Correlation Coefficient Sig. (2-tailed) N	0.281** 0.000 235	-0.001 0.988 206	-0.014 0.831 227
** Correlation is significant at the 0.01 level			

Table 17. Bivariate correlations about Facebook

The results of the bivariate correlations that are summarized in table 17 show that there is a significant positive correlation between the surveillance critique index and the surveillance knowledge index on the one hand and the Facebook knowledge index on the other hand. This result confirms that surveillance parameters have an influence on the usage of ISNS. But nonetheless critical information behaviour on Facebook and knowledge about Facebook are rather small because Facebook is not so much known, and not so much discussed in personal conversations and in the public. Therefore the influence of the surveillance parameters remains limited.

7.6. Usage of MySpace

15.9% of the respondents in our survey use MySpace (figure 34). This is a much lower number than in the case of studiVZ (88.3%) and a lower number than in the case of Facebook (39.5%). We combined the answers to four questions that tested the users' knowledge about what MySpace is allowed to do with their data in order to calculate the MySpace Knowledge Index (figure 35) (0=no correct answer, 1=one correct answer, 2=two correct answers, 3=three correct answers, 4=four correct answers). 15.8% of the MySpace users in our survey have high knowledge of MySpace, 34.7% have good knowledge of MySpace, 43.2% have average knowledge of MySpace, 6.3% have small knowledge of MySpace, and 0% have no knowledge of MySpace. So 50.5% of the MySpace users in our survey have high or good knowledge of MySpace, whereas the remaining 49.5% have average, little, or no knowledge of the platform. In the case of Facebook, 34.1% of the users had a good or high degree of knowledge about what Facebook is allowed to do with their data, whereas in the case of studiVZ users the degree of correct answers to such questions was on average 88.7% (the average of 91.8% and 85.6%). The data show that there is a large difference between the

knowledge that users have on studivZ and the knowledge that they have about MySpace and Facebook. That users know so much about studivZ and not so much about MySpace and Facebook can best be explained by the fact that there is more private and public debate about studivZ because it is the most used ISNS in Austria and Germany and by the negative media coverage and the online information campaign that emerged when studivZ changed its terms of use at the beginning of 2008 so that more surveillance and less privacy became possible.

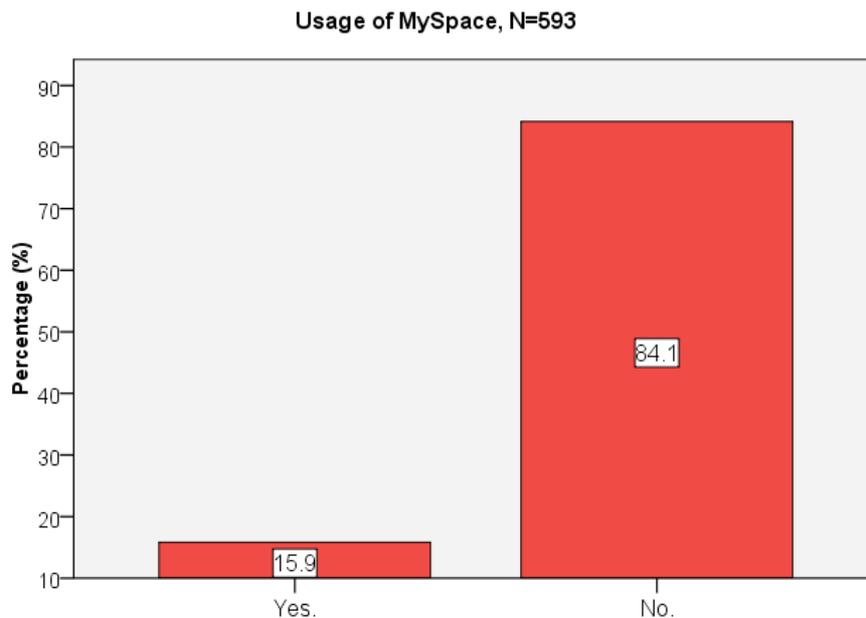


Figure 34. Usage of MySpace

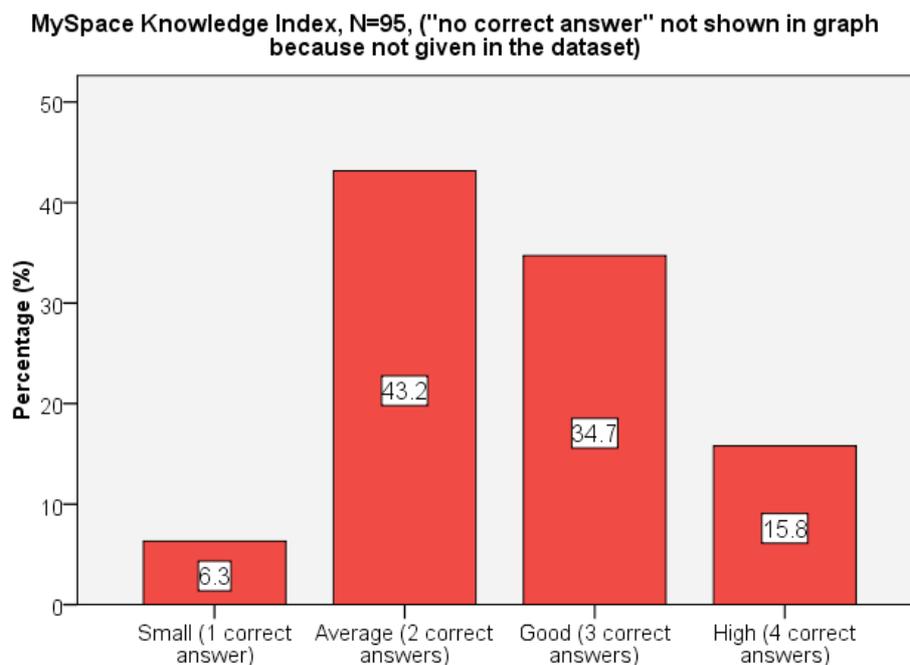


Figure 35. MySpace knowledge index

85.2% of the MySpace users in our survey have activated personalized advertising (figure 35), 69.7% allow all advertising companies to send them ad messages (figure 36). This means that on average 22.6% opted out of advertising options on MySpace. In comparison, on average 67.4% of the users in our survey have opted out of advertising option on studiVZ and on average 35.9% of the users opted out of these options on Facebook. That users are much more critical towards advertising on studiVZ than on MySpace and Facebook can be explained by the fact that the advertising and economic surveillance practices of studiVZ have been a public and interpersonal topic that affected studiVZ's image negatively, when the platform changed its terms of use at the beginning of 2008. MySpace and Facebook are much less used, known, and discussed in Austria and Germany than in other countries like the USA or the United Kingdom.



Figure 36. MySpace information behaviour #1

MySpace Information Behaviour #2: Receiving ads by advertising companies, N=89

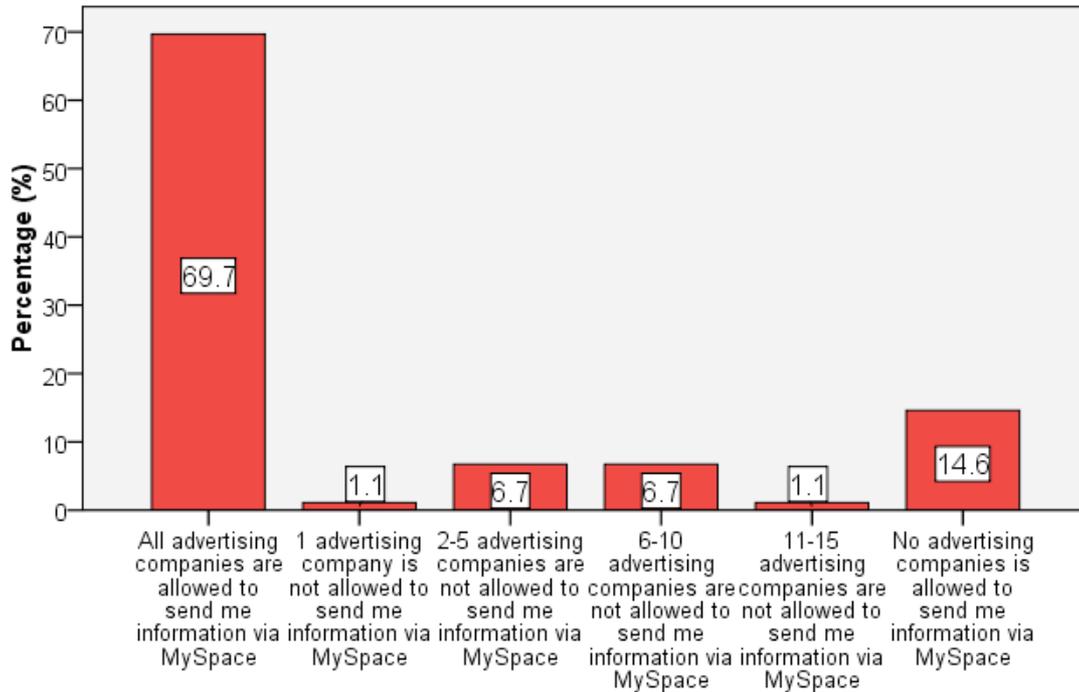


Figure 37. MySpace information behaviour #2

Table 18 shows that there is no significant correlation between general usage behaviour of ISNS or surveillance critique and knowledge on the one hand and knowledge about MySpace or information behaviour on MySpace on the other hand.

	MySpace Knowledge Index	MySpace Information Behaviour #1	MySpace Information Behaviour #2
Usage Intensity ISNS:			
Correlation Coefficient	0.059	0.151	0.140
Sig. (2-tailed)	0.569	0.161	0.190
N	95	88	89
Read Terms of Use:			
Correlation Coefficient	0.053	-0.036	-0.089
Sig. (2-tailed)	0.610	0.534	0.404
N	95	88	89
Surveillance Critique Index:			
Correlation Coefficient	0.074	0.196	-0.159
Sig. (2-tailed)	0.478	0.068	0.136
N	95	88	89
Surveillance Knowledge Index:			
Correlation Coefficient	0.012	-0.027	0.191
Sig. (2-tailed)	0.910	0.805	0.073
N	95	88	89
** Correlation is significant at the 0.01 level			

Table 18. Bivariate correlations about MySpace

7.7. Advantages and Disadvantages of Social Networking Sites

We asked the respondents what they think the greatest advantages and disadvantages, i.e. opportunities and risks, of social networking sites were with the help of two open questions. We received 557 qualitative answer texts to the question that addressed advantages and 542 texts relating to disadvantages. The open questions were asked more at the beginning of the questionnaire before the topic of surveillance was introduced in order to make sure that the respondents were not influenced by this topic in listing advantages and disadvantages. We identified 18 categories for the advantages and 16 categories for the disadvantages and analyzed the answers to the two open questions by content analysis (Krippendorff 2004) so that each text was mapped with one or more categories. Our respondents tended to list more than one major advantage and disadvantage. Therefore each answer was mapped with more than one category in most cases.

Figure 38 presents the major advantages of social networking sites that our respondents mentioned.

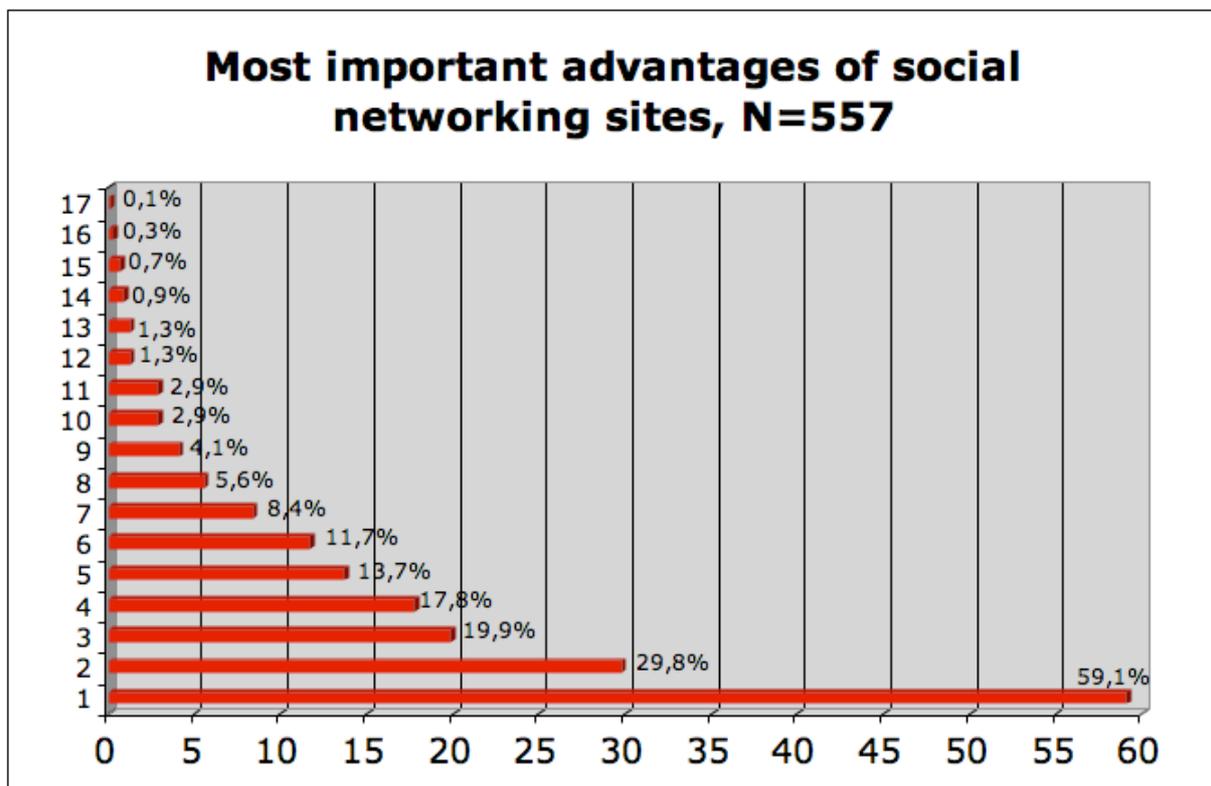


Figure 38. Major perceived opportunities of social networking sites

- 1: Maintaining existing contacts, friendships, family relations, etc
- 2: Establishing new contacts with unknown people or with people whom one hardly knows and can easier contact online
- 3: Finding and renewing old contacts
- 4: Communication in interest groups and hobby groups
- 5: Communication and contacts in general (no further specification)
- 6: International and global character of communication and contacts
- 7: Sharing and accessing photos, music, videos
- 8: Entertainment, fun, spare time, amusement

- 9: Source of information and news
- 10: Browsing other profiles, "spying" on others
- 11: Free communication that saves money
- 12: Reminder of birthdays
- 13: Business communication, finding jobs, self-presentation for potential employers
- 14: Being hip and trendy
- 15: Mobility, access from anywhere
- 16: Self-presentation to others (for non-business reasons)
- 17: Flirting, sex, love

Our survey shows that communication is the most important advantage that the students in our survey mention. Communication for them is more important than self-presentation, sharing images or videos, or getting information. Maintaining existing friendships, family contacts, etc. with the help of social networking sites is the most important advantage that the students in our survey mention. 59.1% of them consider it as a major advantage. 29.8% say that establishing new contacts is very important, 19.9% mention finding and renewing old contacts and friendships as major advantage. 17.8% say that communication in interest and hobby groups is very important. The students in this context especially stress communication about their field of study, university courses, and exams with other students on studiVZ and the possibility of joining music fan groups, learning about new music, and communicating with fans of music groups that one likes on MySpace. 13.7% say that communication in general (without any further classification) is the major advantage. 11.7% stress that social networking sites allow them to establish and maintain international or global contacts across large spatial distances. 8.4% mention sharing photos and other media with friends and accessing such media as major opportunity. 5.6% say that an important aspect of social networking sites is that they are fun and provide entertainment.

Overall these results show maintaining existing contacts is more important than establishing new contacts or renewing old contacts on social networking sites. Maintaining the existing social network and broadening it together form core activities on social networking sites. They are at the same time social network sites and social networking sites. Maintaining the existing network is a reproduction process, each time one communicates with existing friends and contacts, one reproduces autopoietically the existing network. The network lives through permanent renewed networking, therefore no clear distinction between network and networking can be drawn and one can either speak of social networking sites or social network sites. Each network is based on permanent reproductive networking, friendship work is needed for keeping ones network working. Establishing new network contacts as process of expansive networking is embedded into existing networks. Networking makes a network working as expanding community of social relations.

Here are some characteristic examples of answers that were given to the question of what the major advantages of social networking platforms are:

Number of data set	Categories	Answer (English)	Answer (German)
#40	2, 3, 10, 16	Finding old contacts, inspecting other people, self-propaganda,	verlorene Leute wiederfinden, Leute inspizieren können,

		finding interesting people	Selbstpropaganda, interessante Menschen finden
#47	1	Remaining in contact after a joint period of studying, collaboration, a journey or simply a period of more intensive contact has come to an end, e.g. after relocating etc. You also know ears later how/where to find people.	Kontakt halten nachdem eine gemeinsame Studienphase, Zusammenarbeit, Reise oder einfach Zeit eines intensiveren Kontaktes vorbei ist, z.B. nach einem Umzug o.ä. Man weiß auch Jahre später noch, wie/wo man die Leute findet.
#81	1, 2	Due to anonymity you can make contacts more easily, respectively you can also write to people whom you do not know that well (from university courses, if you have questions about university, etc...). It is easier to stay in contact with friends who are currently abroad or live abroad.	durch die Anonymität kann man leichter Kontakt schließen, bzw, auch weniger bekannte Personen anschreiben (aus Lehrveranstaltungen, wenn man Fragen hat bzgl. der Uni etc...). Es ist leichter, mit Freunden in Kontakt zu bleiben, die gerade im Ausland sind oder überhaupt im Ausland leben.
#82	1	You have all your friends in one spot, you do not permanently have to ask for mobile phone numbers	man hat alle freunde auf einem fleck, muss nicht ständig nach Handynummer oder dergleichen fragen
#93		You can find old acquaintances and stay in touch with them. I have also already contacted students in order to co-operate with them in various seminars and internships.	Alte Bekannte wieder finden, den Kontakt mit Ihnen aufrecht erhalten, Habe auch schon Studienkollegen zwecks Zusammenarbeit in diversen Seminaren und Praktika angeschrieben.
#97	6	International coming together	international coming together
#104	1	Such platforms make it easier to stay in contact also across larger distances – for example with former schoolmates.	Solche Plattformen erleichtern es, auch über größere Distanzen in Kontakt zu bleiben - bspw. mit ehemaligen Schulkollegen.
#118	8, 9, 10	Interesting way of spending time, you can find out a lot about other people whom you only know casually, you stay informed what others are doing at the moment	Interessanter Zeitvertreib, man kann viel über Leute herausfinden, die man nur beiläufig kennt, Kontakt halten, bleibt informiert was andere gerade tun
#123	2, 3, 6	Connects people from all over the world and you find old and new friends	Verbindet Leute aus aller Welt und man findet alte und neue Freunde
#155	1, 2, 10	You can stay in contact with old school mates. You can read and see what your fellow students are doing in their spare time. You can introduce yourself to other users – “Hello, here I am and I want to get in contact with you”. Boosting of voyeurism.	Kontakt halten mit alten Schulfreunden. Lesen und sehen, was Mitstudenten in der Freizeit treiben. Sich den anderen Nutzern vorstellen - "Hallo da bin ich und ich will mit dir in Kontakt treten." Voyeurismus ankurbeln
#165	1, 3, 4	“Recovering” acquaintances; easy way for staying in touch, exchanging	Bekannte "wiederfinden"; einfache Möglichkeit, in Kontakt zu bleiben,

		opinions (e.g. in "discussion groups"), finding like-minded people (e.g. in the rubric images...)	Meinungsaustausch (z.B. in den "Gruppen"), Gleichgesinnte finden (z.B. unter der Rubrik Fotos...)
#190	1, 4	You cannot even study without studiVZ. It is almost courteous and it is much more difficult to stay in touch without it.	ohne studivz kann man schon gar nicht mehr studieren. gehört schon fast zum guten ton und ohne ist kontakte aufrecht erhalten weitaus schwieriger
#199	2	It is easy to establish contact with colleagues that you have thus far hardly known. Especially in cases where one has not-yet exchanged mobile phone numbers, but you need something from each other.	Leichter Kontakt zu bis dahin fast unbekanntem Kollegen. Gerade wenn man noch keine Handynummern ausgetauscht hat, aber etwas voneinander braucht.
#246	1, 2, 4, 8, 16	Finding and meeting friends, entertainment and amusement, communities, self-presentation, learning to know new people	Freunde treffen und finden, Unterhaltung und Zeitvertreib, Communities, Selbstdarstellung, neue Leute kennen lernen
#267	1, 2	To come in touch or stay in touch with people that have the same interests as you; you can build up a small network of friends and acquaintances; finding others and being found	mit Leuten, die selbe Interessen haben, in Kontakt treten bzw. bleiben; man kann ein kleines Netzwerk an Freunden/Bekanntem aufbauen; finden und gefunden werden
#275	3, 4	Meeting people with similar interests, recovering contacts with old school mates or former friends, communication about courses among students (on studiVZ), sharing hobbies and spare time activities with other people.	Kennenlernen von Leuten mit ähnlichen Interessen, Kontakte wiederherstellen zu alten Schulkollegen, ehem. Freunden, Austausch unter Studierenden über best. Lehrveranstaltungen (bei studiVZ), seine Hobbies und Freizeitbeschäftigungen mit anderen Leuten zu teilen.
#283	1, 3, 4, 7	You can meet old school friends on studiVZ, it is easier to stay in touch with "acquaintances". MySpace is a brilliant publishing opportunity for bands (uploading MP3s, announcing concert dates). Event managers nowadays ask more frequently about your MySpace address than about your "normal" homepage because the first is more compact. MP3s, press releases, musical influences, images: all that an event manager wants to know respectively that is all s/he needs to know.	Bei Studivz alte Schulfreunde wieder finden, Kontakte zu "Bekanntem" lassen sich leichter halten. MySpace ist eine hervorragende Publikationsmöglichkeit für Bands (MP3s online stellen, Konzerttermine bekannt geben). Konzertveranstalter fragen mittlerweile öfter nach der MySpace Adresse als nach der "normalen" Homepage, weil Erstere einfach kompakter ist. MP3s, Presstext, Einflüsse, Fotos: mehr will ein Veranstalter nicht wissen bzw. mehr braucht er nicht.
#291	1	Staying in contact with people abroad (relatives in Bremen, friends in Alaska, Spain and the United Kingdom, but also friends in Austria who write small messages in	Kontakt zu halten zu Menschen in der Ferne (Verwandte in Bremen, Freunde in Alaska, Spanien und Großbritannien, aber auch Freunde in Österreich, die zwischendrin

		between if there is no time for calling on the phone)	kleine Nachrichten schreiben, wenn keine Zeit zum Telefonieren ist).
#377	4	Networking of students, exchange between like-minded people	Vernetzung der StudentInnen untereinander, Austausch von Gleichgesinnten
#641	2, 8, 9, 13	You can quickly get into contact with other people, you find information on for example university courses (studiVZ), nice way of spending time, you can present yourself for job applications on Xing	man kann schnell mit anderen Leuten in Kontakt treten, man findet eventuell Informationen beispielsweise zu einem Uni-Kurs (studiVZ), netter Zeitvertreib, man kann sich selbst darstellen - bei Xing für Bewerbungen ...

Table 19. Examples for advantages that were listed by the respondents

Figure 42 presents the major disadvantages of social networking sites that our respondents mentioned.

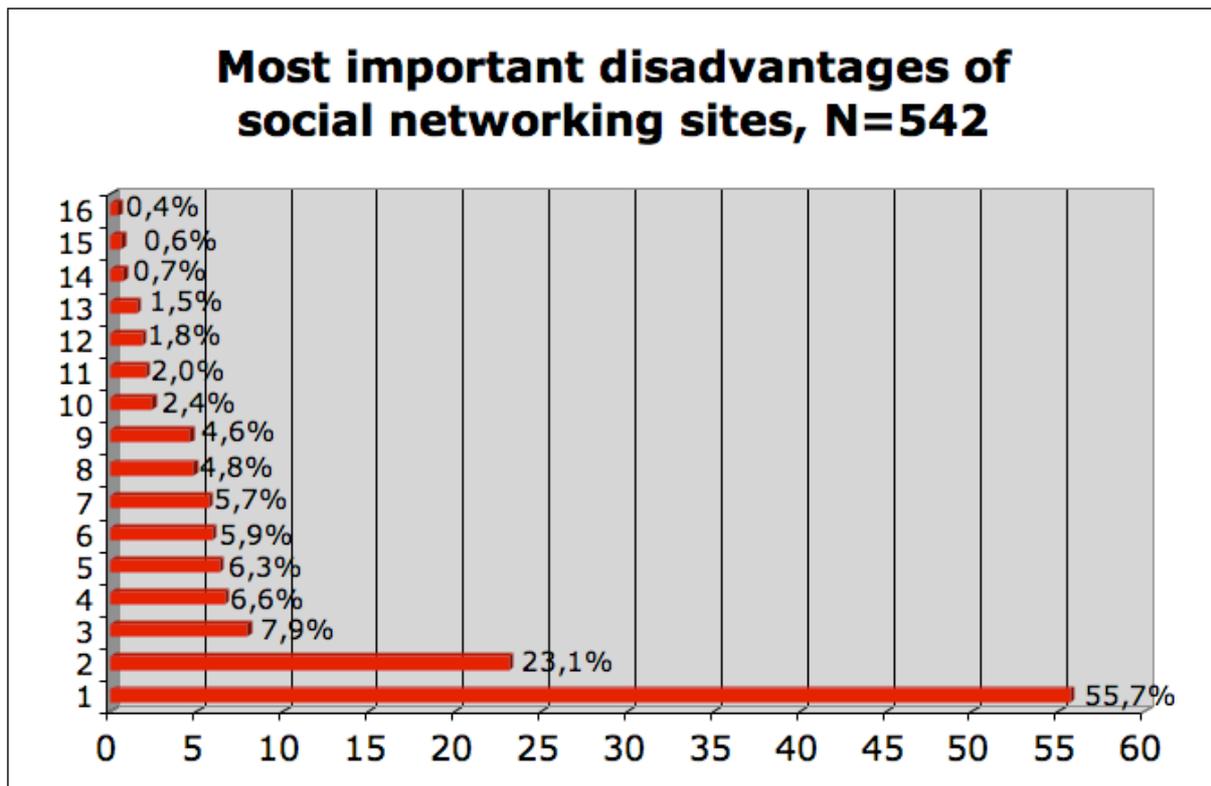


Figure 39. Major perceived risks of social networking sites

- 1: Data abuse or data forwarding or lack of data protection that lead to surveillance by state, companies, or individuals
- 2: Private affairs become public and result in a lack of privacy and privacy control
- 3: Personal profile data (images, etc) are accessed by employer or potential employers and result in job-related disadvantages (such as losing a job or not getting hired)
- 4: Receiving advertising or spam
- 5: Lack or loss of personal contacts, superficial communication and contacts, impoverishment of social relations
- 6: Stalking, harassment, becoming a crime victim
- 7: Commercial selling of personal data

- 8: Data and identity theft
- 9: I see no disadvantages
- 10: It is a waste of time
- 11: Virus, hacking and defacing of profiles, data integrity
- 12: Internet addiction, increase of stress and health damages
- 13: Unrealistic, exaggerated self-presentation, competition for best self-presentation
- 14: Disadvantages at university because professors can access profiles
- 15: Costs for usage can be introduced (or exist in the case of some platforms)
- 16: Friends can get a negative impression of me

55.7% of the respondents say that political, economic, or personal surveillance as a result of data abuse, data forwarding, or a lack of data protection is a main threat of social networking sites. 23.1% say it is problematic that personal affairs that should better be kept private and should not be known by others tend to become public on social networking sites. 7.9% say that it is a danger that also current and potential employers can access profiles, which could result in job-related disadvantages such as not getting a job or losing a job. 6.6% express concern about advertising or spam on social networking platforms. 6.3% say that personal contacts tend to get lost, impoverished or tend to become superficial as a result of social networking platforms. 5.9% argue that unwanted contacts, stalking, harassment and becoming a potential crime victim are major risks of social networking platforms. 5.7% mention that it could be that their personal data is sold to third parties.

Here are some characteristic examples of answers that were given to the question of what the major disadvantages of social networking platforms are:

Number of data set	Categories	Answer (English)	Answer (German)
#6	1	Big Brother is watching you.	Big Brother is watching you
#13	1	The "transparent individual": everybody knows everything about everyone	Der „gläserne Mensch“: jeder weiß alles über jeden.
#65	3	Spying by employers	Schnüffelei von Arbeitgebern
#79	2	The whole world can participate in my private life if I do not set limits or controls	die ganze Welt kann an meinem Privatleben teilhaben, wenn ich es nicht einschränke/selber kontrolliere
#93	1, 4, 7	My data are sold for advertising. You become too "transparent" for strangers.	Dass meine Daten für Werbung verkauft werden, dass man zu „durchsichtig“ für Fremde wird.
#106	2	Too much invasion into my privacy	Dringt zu tief in meine Privatsphäre ein
#109	7	Personal data are sold to different corporations.	Die persönlichen Daten werden zu unterschiedlichen Firmen verkauft.
#125	1, 13	It is problematic to find out so much about others, although you do not know them! Apparently many people	Dass man so viel über Leute in erfahrung bringen kann, obwohl man diese nicht kennt! Anscheinend

		<p>have such complexes that they think they must distinguish themselves from others by many pictures and by details from their private lives!!! Furthermore I find it interesting respectively very alarming that many members write messages to each other by using the public pinboard that can be read by everybody instead of using the normal message options.</p>	<p>haben viele Menschen solche Komplexe, dass diese meinen, sie müssen sich mit vielen Fotos von sich selbst und Details aus deren Privatleben profilieren!!! Außerdem finde ich es interessant bzw. Sehr besorgniserregend, dass viele Mitglieder sich Nachrichten über das Gästebuch schreiben, welches von jedem eingesehen werden kann, anstatt die normale Nachrichtenoption zu nutzen.</p>
#126	3	<p>I find it problematic when other people upload images that show myself in an unfavourable position, for example with a glass of beer or in a bikini – a potential employer could be bothered.</p>	<p>Wenn andere Menschen Fotos online stellen, die mich in einer wenig vorteilhaften Position zeigen, zb mit einem Bierglas, im Bikini – ein potenzieller Arbeitgeber könnte sich daran stören.</p>
#155	2, 3	<p>Users disclose their private lives to the whole world. It can happen that I am judged by my online profile and the images that I am linked with if I apply for a job.</p>	<p>Dass die Nutzer ihr Privatleben der ganzen Welt offenbaren. Bei der Bewerbung um einen Job nach dem Profil und den Fotos auf die ich verlinkt bin zu beurteilt werden.</p>
#173	1, 5, 13	<p>I find the enormous self-presentation troubling. "I am beautiful, interesting, and popular". Superficiality (Having a friends list that is as large as possible); troubling is also the possibility to find out very much about other persons, although that is none of my business (linked images, user status, pin board entries).</p>	<p>Die enorme Selbstdarstellung: „Ich bin hübsch, interessant, beliebt“. Oberflächlichkeit (eine möglichst große Freundesliste zu haben); die Möglichkeit sehr viel über andere Personen rausfinden zu können, was mich/andere eigentlich gar nichts angeht (über verlinkte Bilder, Statustexte, Gästebucheinträge...)</p>
#198	9	<p>There are no disadvantages because I would never enter data that could sometime be used negatively against me.</p>	<p>Keine, denn ich würde nie Daten angeben die möglicherweise irgendwann negativ gegen mich verwendet werden könnten.</p>
#224	1, 2, 7	<p>Data surveillance, the transparent human, strangers gain insights into privacy, selling of private data and browsing behaviour</p>	<p>Datenverfolgung, Gläserner Mensch, privater Einblick durch Fremde, Weiterverkauf privater Daten und Surfverhalten</p>
#228	1	<p>The transparent human</p>	<p>Gläserner Mensch</p>
#261	6	<p>Meeting psychopaths</p>	<p>Psychopathen treffen</p>
#366	1, 5, 6, 7, 12	<p>Who owns the information (data, images, etc)? Surveillance (also by other members). Who guarantees that my flat is not robbed while I am on a holiday (if for example I announce this with my mood message on Facebook...), you can loose the connection to others, stress (how many hours online, updating?)</p>	<p>Wem gehören die Informationen? (Daten, Fotos, etc) Überwachung (auch durch andere Mitglieder) Wer garantiert, dass meine Wohnung nicht ausgeraubt wird, während ich auf Urlaub bin (und das auch bspw. Über meine Moodmessage in Facebook ankündige...), Anschluss zu verlieren, Stress (wieviele Stunden online, updating?)</p>
#393	3	<p>The danger is that an employer takes a look at it and that a job opportunity</p>	<p>Dass der Arbeitgeber auch da rein schaut und man sich trotz tollen CV</p>

		gets "fucked up" although you have a great CV and a great job interview.	und Vorstellungsgespräch die Jobchance „versaut“
#409	1	To be "spied on" by a third party	von Dritten „ausespioniert“ werden
#454	1	The surveillance society	Überwachungsstaat
#459	1	That others spy on me	dass Leute mir nachspionieren
#531	1, 2	Privacy, transparent identity	Privatsphäre, gläserne Identität
#604	5	I think the greatest danger is to lose contact to the "real" world and to discontinue or strongly minimize the real contact to friends.	Ich denke die größte Gefahr besteht darin, den Kontakt zur "wirklichen" Welt zu verlieren und den realen Kontakt zu Freunden abzubrechen oder stark zu minimieren.
#650	6	Stalking	Stalking
#657	1, 5, 10	The transparent individual! Uses no longer have time for friends, contemplation, family and other really important things, etc, but are rather busy all day to add, to actualize and to answer comments, etc.	Der gläserne Mensch! Die Nutzer haben keine Zeit mehr für Freunde, zum Nachdenken, für Familie und wirklich wichtige Dinge etc, sondern sind den ganzen Tag damit beschäftigt, zu adden, zu aktualisieren und auf Kommentare usw zu antworten

Table 20. Examples for disadvantages that were listed by the respondents

The data of our survey show that 59.1% consider maintaining existing contacts and 29.8% establishing new contacts as major advantage of social networking sites, whereas 55.7% say that surveillance as a result of data abuse, data forwarding, or a lack of data protection is a major threat of such platforms. Communication and the resulting reproduction and emergence of social relations are overwhelmingly considered as major advantage, potential surveillance overwhelmingly as major disadvantage. The impression of the majority of the respondents is that social networking sites enable communicative advantages that are coupled with the risk of surveillance and reduced privacy. How can we explain that they are willing to take the surveillance risk that they are knowledgeable and conscious about? Communication and surveillance are antagonistic counterparts of the usage of commercial social networking platforms: Our data show that students are heavily using social networking sites and are willing to take the risk of increased surveillance although they are very well aware of surveillance and privacy risks. The potential advantages seem to outstrip the potential disadvantages. It is not an option for them not to use social networking platforms because they consider the communicative and social opportunities associated with these technologies as very important. At the same time they are not stupid, uncritical, or unaware of potential dangers, but rather very conscious of the disadvantages and risks. They seem to fear that they miss social contacts or will have disadvantages if they do not use platforms such as studivZ, Facebook, MySpace. Not using these technologies or stopping using them is clearly not an option for most of them because it would result in disadvantages such as reduced social contacts and the feeling of not participating in something that has become important for the young generation. The crucial aspect of the antagonism between communicative opportunities and the surveillance risk is that alternative social networking platforms that are non-

commercial and non-profit and therefore do not have an interest in economic surveillance and that see privacy as a fundamental right that needs to be well-protected under all circumstances, are hardly available or hardly known. Commercial profit-oriented sites such as studivZ, Facebook, or MySpace have reached a critical mass of users that is so large that these commercial providers have become cultural necessities for most young people. For non-commercial platforms, it is hard to compete with these economic corporations because the latter have huge stocks of financial means (enabled by venture capital or parent companies such as News Corporation or Holtzbrinck), personnel, and technological resources. Capitalist business interests and the unequal distribution of assets that is characteristic for the capitalist economy result in the domination of markets by a handful of powerful corporations that provide services and that make influence by non-commercial, non-profit operators difficult. Given the fact that students are knowledgeable of the surveillance threat, it is obvious that they are willing to use alternative platforms instead of the major corporate ones, if such alternatives are available and it becomes known that they minimize the surveillance threat. Not students are to blame for potential disadvantages that arise from their usage of social networking platforms that in the opinions of our respondents threaten privacy and advance surveillance, but the corporations that engage in surveillance and enable surveillance are to blame. Corporate social networking platforms are for example not willing to abstain from surveillance for advertising because they have profit interests. The antagonism between communicative opportunities and the surveillance threat is not created by students' and young people's usage of social networking platforms, but by the economic and political logic that shapes social networking corporations' platform strategies.

7.8. The Usage Rate of Social Networking Platforms in Comparison

Figure 42 shows the share of users in our sample in different platforms that were considered as being "social networking platforms" by the respondents. There is a large concentration of users on studivZ (88.3% of the respondents), which implies that there is also a market concentration with one dominant actor. Other important platforms are Facebook (39.5%), MySpace (15.9%), Xing (9.0%), Lokalisten (7.4%), and Szene1 (4.3%). The remaining 61 platforms that were mentioned in our survey, each reach less than 1% of the respondents. This means that among the 67 platforms listed by the respondents, we find one large platform, 5 medium-sized ones, and 61 small ones. These data give reason to assume that profit distribution in the social networking market is highly centralized.

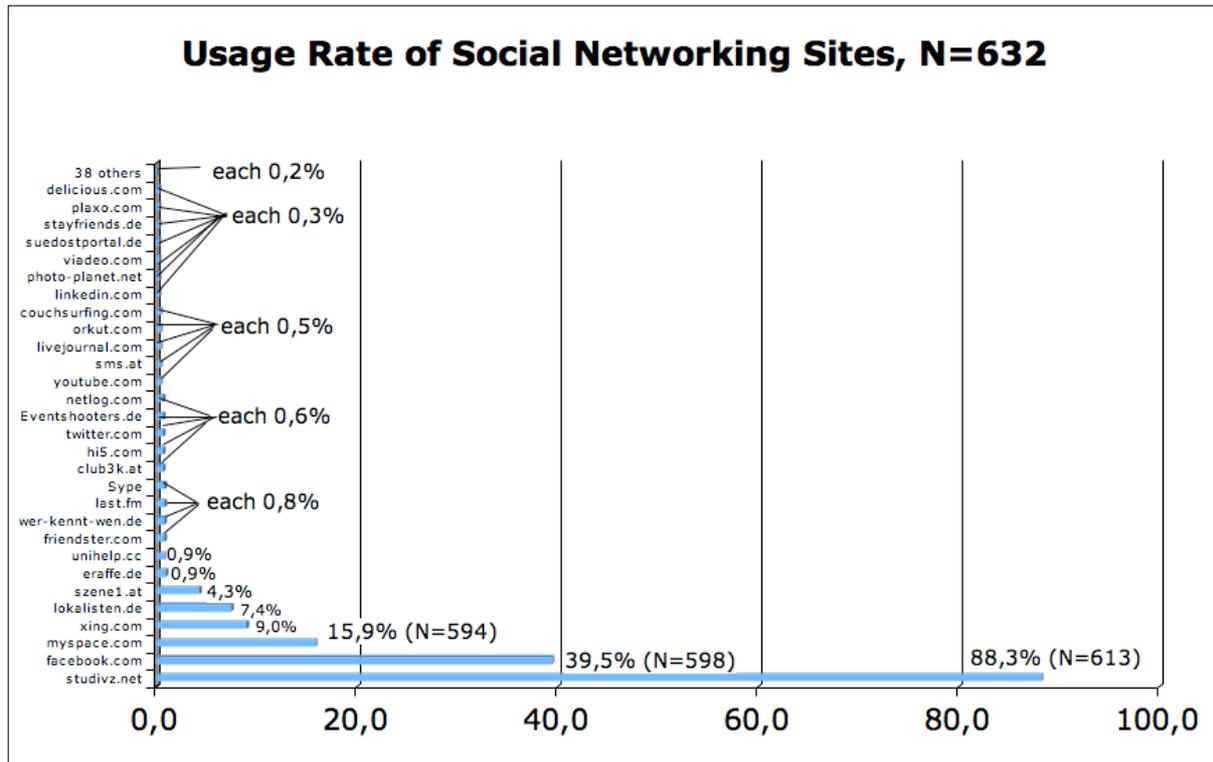


Figure 40. Comparison of the usage rate of social networking platforms

8. Implications and Conclusions

In this section, we will discuss some political conclusions of our study. The implications and conclusions are organized along the five research questions that were introduced in section 6.

- (1) What do students consider as the greatest opportunities of ISNS?
- (2) What do students consider as the greatest risks of ISNS?

We asked the respondents what they think the greatest advantages and disadvantages, i.e. opportunities and risks, of social networking sites were with the help of two open questions.

Maintaining existing friendships, family contacts, etc. with the help of social networking sites is the most important advantage that the students in our survey mention. 59.1% of them consider it as a major advantage. 29.8% say that establishing new contacts is very important, 19.9% mention finding and renewing old contacts and friendships as major advantage. Maintaining existing contacts seems to be more important than establishing new contacts or renewing old contacts on social networking sites.

55.7% of the respondents say that political, economic, or personal surveillance as a result of data abuse, data forwarding, or a lack of data protection is a main threat of social networking sites. 23.1% say it is problematic that personal affairs that should better be kept private and should not be known by others tend to become public on social networking sites.

The data of our survey show that 59.1% consider maintaining existing contacts and 29.8% establishing new contacts as major advantage of social networking sites, whereas 55.7% say that surveillance as a result of data abuse, data forwarding, or a lack of data protection is a major threat of such platforms. Although students are very well aware of the surveillance threat, they are willing to take this risk because they consider communicative opportunities as very important. That they expose themselves to this risk is caused by a lack of alternative platforms that have a strongly reduced surveillance risk and operate on a non-profit and non-commercial basis.

- (3) How knowledgeable are students of the rise of a surveillance society?

We asked questions about the judicial situation of surveillance in Austria and Europe, including questions about the increased surveillance options available to the police due to the amendment of the Austrian Security Police Act and the introduction of the European Data Retention Directive. With the help of these questions, we calculated a surveillance knowledge index. 81.8% of the students in our survey had no or only little knowledge about surveillance, whereas 18.3% had a good or high degree of knowledge about surveillance. The median of the surveillance knowledge index is 1 (little knowledge of surveillance). Gender, class, income, and location stratify student's knowledge about surveillance. Being female and having a white-collar father increase the possibility of having low surveillance knowledge, being male, higher income, and living or coming from a larger city increases the possibility of having a high degree of

surveillance knowledge.

It is certainly desirable that young Austrians have good knowledge of the political situation in Austria and Europe. In order to increase the degree of conscious knowledge about surveillance, we suggest that critical educators, critical scholars, social movements, consumer groups, data protection specialists/groups, consumer protection specialists/groups, critical citizens' initiatives, unions, critical media, critical politicians, and political parties that are critical of surveillance present the topic of the surveillance society in the public, in educational courses, the media, and especially in addressing young people as a central problem of contemporary society that threatens democracy and human rights. Students in most societies are the most well informed and most critical citizens. If they only have a low degree of knowledge about surveillance, then this is an alarm signal that is an indication that there is little such knowledge in the overall population, too, and that there is a lack of critical public discourse on the issue. Such public awareness initiatives might remain limited, if there are powerful institutions and actors that have an interest in forestalling critical public debates on surveillance due to economic or political interests. Nonetheless, to try to strengthen public debate is the only way of struggling for improvements.

(4) How critical are students of the rise of a surveillance society?

We combined the answers to five scaled questions to an overall surveillance critique index that can take on values between zero and twenty-five (0: no critical consciousness on surveillance, 25: very critical of surveillance). The statistical average of this index is 17.3. 67.4% of the respondents are critical or rather critical of surveillance. Critique of surveillance is stratified by gender, field of study, number of semesters studied, income, and usage frequency of ISNS. Being female, studying natural sciences, and high usage of ISNS increase the probability to be uncritical of surveillance, whereas being male, studying social sciences, having higher income, and being a graduate or doctoral student increases the likelihood that students are critical of surveillance. 58.9% agree or agree strongly that state surveillance has increased after 9/11. 58.1% agree or strongly agree that you have to be afraid of surveillance even if you have nothing illegal to hide. But critique towards surveillance seems to be diffuse. Most know that surveillance is problematic, can threaten privacy, undercut democracy, and pave the way towards a totalitarian society, but there is little knowledge about the actual juridical situation in Austria and Europe.

There is a general critical attitude of students towards surveillance combined with little knowledge about surveillance. If there is a critical basic attitude, then it is likely that citizens will act politically once they feel alarmed by public discussions. Therefore given such a condition, political discourse is easier and promises to be more successful than in situations where there is little critical consciousness on a certain topic. Therefore it is quite likely that a certain degree of students will join citizens' initiatives and act politically if they gain more knowledge about actual surveillance. Our recommendation is therefore that critical educators, critical scholars, social movements, consumer groups, data protection specialists/groups, consumer protection specialists/groups, critical citizens' initiatives, unions, critical media, critical politicians, and political parties that are critical of surveillance present the topic of the surveillance society on a very concrete level that shows how citizens are immediately affected by

surveillance by engaging in activities such as using the Internet, using social networking sites, using mobile phones, leaving data traces in everyday life, etc.

The most successful strategy for strengthening public discourse on an issue is to try to organize campaigns that tackle political issues and show how citizens are immediately negatively affected by certain political conditions. Public campaigns can certainly have limits, especially if there are dominant institutions and actors that have opposing views and have strong influence on the media and public discourse by political and economic power. Therefore one should not be overoptimistic concerning the possibilities and perspectives for organizing critical discourse in a society that is economically and politically stratified, i.e. shaped by economic and political power differentials. Nonetheless, the only way to bring about change is to try to organize collective articulations of discontent with certain situations.

Our study shows that there is a certain basic critical attitude towards surveillance by students. Students tend to be the most critical citizens in a society. It is certainly a limit that we do not know more about the attitudes towards and knowledge about surveillance of non-students. We cannot draw inferences from students' consciousness and knowledge to the rest of the population. It is a task for future research to find out more about knowledge about and critical awareness of surveillance of citizens who have a non-student status.

(5) How does the degree of knowledge about surveillance and the degree of critical consciousness on surveillance influence the usage of social networking sites?

88.3% of the respondents in our survey use studiVZ, 39.5% Facebook, and 15.9% MySpace. This shows that the situation of the usage of social networking sites is different in German-speaking countries than in other parts of the world. studiVZ is the dominant actor and therefore tends to concentrate a large amount of the economic profits derived from social networking sites in Austria and Europe. This concentration process also gives studiVZ a huge degree of power and control over personal data.

On average, 88.7% of the studiVZ users in our survey know what the corporation is allowed to do and not to do with their data. 50.5% of the MySpace users in our survey have a high or good degree of knowledge about the platform. In the case of Facebook, only 34.1% of the users in our survey have a good or high degree of knowledge about Facebook.

On average, 67.4% have opted out of advertising options on studiVZ, 35.9% opted out of these options on Facebook, and 22.6% opted out of such options on MySpace. The platforms provide such options to different degrees and with different accessibility and usability. Table 21 summarizes the rights and opt-out options of the social networking corporations in our study. On Facebook, it is not possible to opt out of personalized advertising. On MySpace, opting out of personalized advertising and sharing of data with advertising clients is possible, but is almost impossible to find these options because they cannot be accessed in the standard settings, but only by links that one finds in the privacy policy. This might explain the low degree of deactivated advertising options in the case of MySpace.

	studiVZ	Facebook	MySpace
Selling and reuse of user content is allowed		X	
Targeted personalized advertising is allowed	X (opt out)	X (no opt out)	X (opt out)
Sharing of data with third parties is allowed for commercial aims		X (no opt out)	X (opt out)
Reception of advertising emails is allowed	X (opt out)	X	X
Passing on of data to the police for law enforcement or crime prevention	X	X	X

Table 21. Rights guaranteed to corporations by terms of use and privacy policies on studiVZ, Facebook, and MySpace

In our study, the degree of general critical awareness of surveillance (surveillance critique index) is significantly positively correlated with knowledge about studiVZ and critical information behaviour on studiVZ. The degree of general critical awareness of surveillance and the degree of general knowledge about surveillance is significantly positively correlated with the knowledge that students have about Facebook. This shows that there tends to be a relationship between subjective surveillance parameters on the one hand and parameters that concern social networking sites on the other hand.

Our data show that there is a large difference between the knowledge about and information behaviour on studiVZ on the one hand and Facebook and MySpace on the other hand. The students in our survey tend to be well informed about studiVZ and less well informed about Facebook and MySpace. Also they tend to opt out of advertising on studiVZ, but not so much on Facebook and MySpace. This can be explained by the fact that when studiVZ changed its terms of use at the beginning of 2008, there was a public discussion and an information campaign on studiVZ that to a certain degree created a negative public image of studiVZ as being the “SchnüffelVZ” (SniffleDirectory). The online information campaign did not attract a very large number of users and did not make use of cyberprotest strategies such as online petitions. The new terms of use could not be circumvented by the information campaign, which shows that corporate interests in most cases are more powerful than citizens’ interests. But the public and interpersonal discourse about studiVZ and surveillance seem to have caused a concrete critical awareness of young users that led most of them to opt out of personalized advertising and advertising information that is received by email and the studiVZ message service. Facebook and MySpace are much less used, and discussed in Austria and Germany. This explains why users tend to know much less about these platforms and tend to behave rather uncritical on them. In the case of studiVZ, information about the changes in privacy, surveillance, and advertising that studiVZ planned by introducing new terms of use, seems to have activated the critical potential of the students that is present in the form of a general critical attitude towards surveillance so that a majority of students have actively taken steps to limit the amount and type of advertising they receive.

Based on these findings, we recommend that critical citizens, critical citizens’ initiatives, consumer groups, social movement groups, critical scholars, unions, data protection specialists/groups, consumer protection specialists/groups, critical politicians, critical political parties observe closely the relationship of surveillance and corporations and document instances where corporations and politicians take measures that threaten privacy or increase the surveillance of citizens. Such documentation is

most effective if it is easily accessible to the public. The Internet provides means for documenting such behaviour. It can help to watch the watchers and to raise public awareness. In recent years, corporate watch organizations that run online watch platforms have emerged (see figures 41, 42, 43).

Examples are:

CorpWatch Reporting (<http://www.corpwatch.org>),
Transnationale Ethical Rating (<http://www.transnationale.org>),
The Corporate Watch Project (<http://www.corporatewatch.org>),
Multinational Monitor (<http://www.multinationalmonitor.org>),
crocodyl: Collaborative research on corporations (<http://www.crocodyl.org>),
Endgame Database of Corporate Fines (<http://www.endgame.org/corpfines.html>),
Corporate Crime Reporter (<http://www.corporatecrimereporter.com>),
Corporate Europe Observatory (<http://www.corporateeurope.org>),
Corporate Critic Database (<http://www.corporatecritic.org>) .

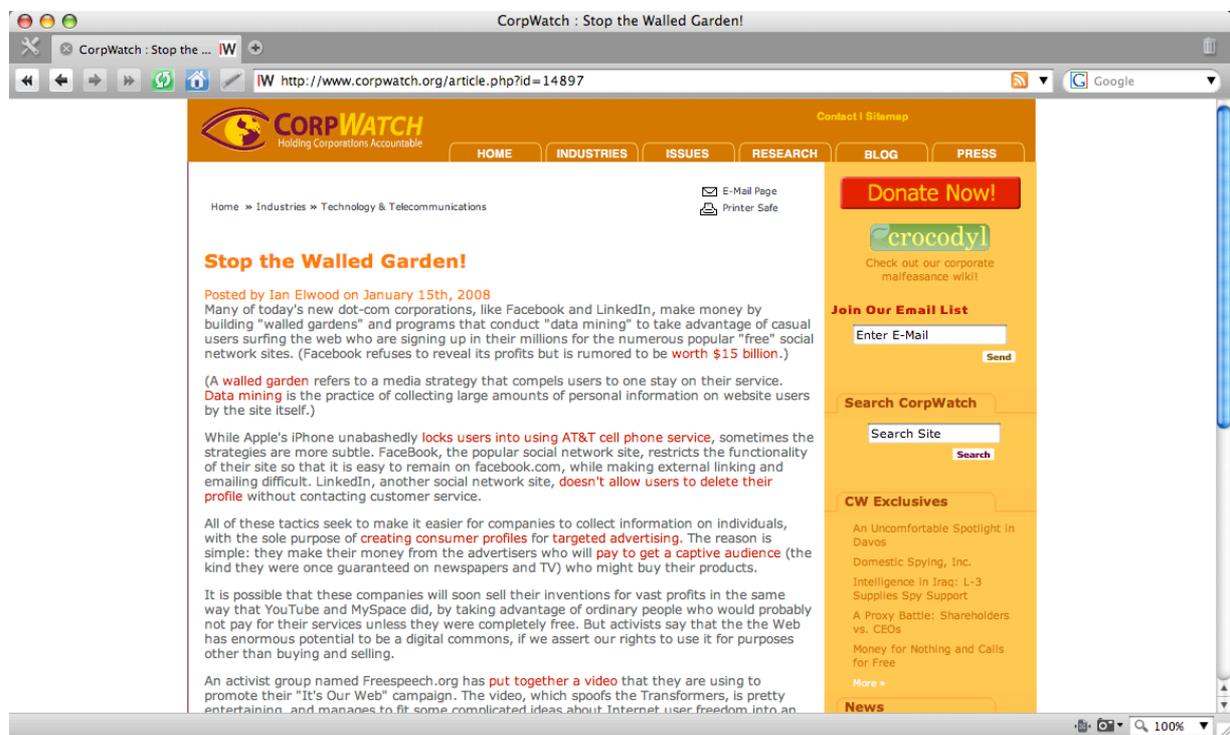


Figure 41. Corporate Watch Organizations: Example 1 (<http://www.corpwatch.org>)

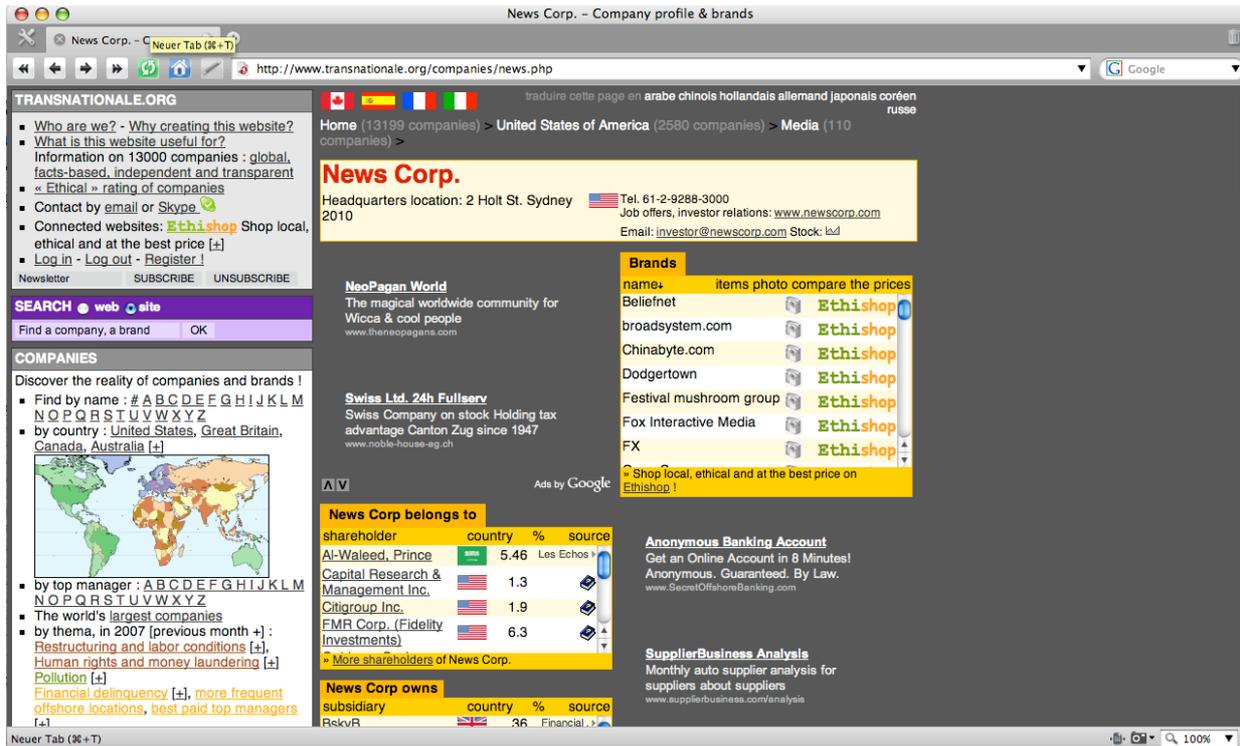


Figure 42. Corporate Watch Organizations: Example 2 (<http://www.transnationale.org>)

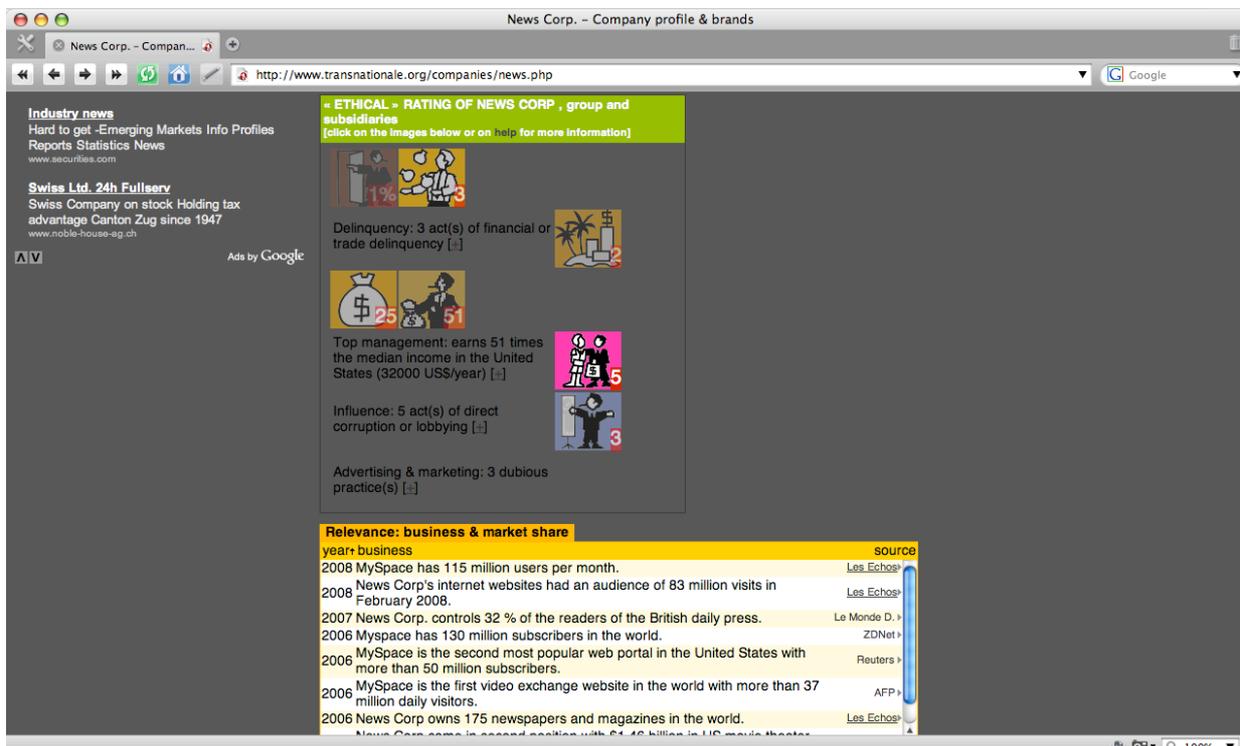


Figure 43. Corporate Watch Organizations: Example 3 (<http://www.transnationale.org>)

These examples show that there are potentials for building counter-hegemonic power that aims at raising critical awareness about certain political issues by watching and documenting what powerful actors, organizations, and institutions are planning and doing. In the case of the topic of surveillance, such citizen initiatives try to build counter-power and counter-hegemony by watching the watchers, surveilling the surveillers. An example for such an initiative in Austria is www.platterwatch.at, a

platform that was created by the Austrian Green Party at the time when the Security Police Act was amended. "PLATTERWATCH documents the creation of the surveillance state and the dismantling of the constitutional state. We collect facts that range from online state surveillance by Trojans or the IMSI-catcher to the activities of the US Homeland Security within Austria. PLATTERWATCH accompanies the Interior Minister [Günther Platter (Austrian People's Party ÖVP) was Austrian Interior Minister from February 28, 2003 until July 1, 2008. He was followed by Maria Fekter (ÖVP)] throughout Austria. We put the minister online"³⁶.

There are certainly limits of watchdog organizations and initiatives. They are generally civil society projects because it is unlikely that big corporations or governments support initiatives that tend to criticize corporations and governments with big amounts of money. Therefore such projects are frequently based on precarious, self-exploitative labour, and are confronted with a lack of resources such as money, activists, time, infrastructure, influence, etc. If political or economic institutions offer support, then there is a danger that they try to influence the activities of such projects, which can severely damage or limit the autonomy and critical facility of such projects. They seem to be trapped in an antagonism between resource precariousness and loss of autonomy that is caused by the fact that the control of resources is vital for having political influence in contemporary society and that resources in this very society are unequally distributed so that corporations and established political actors have much more power and influence than other actors. Given this situation, it would be a mistake not to try to organize citizens' initiatives, but one should bear in mind that due to the stratified character of capitalism it is more likely that such initiatives will fail and remain unimportant than that they will be successful in achieving their goals.

There are no easy solutions to the problem of civil rights limitations due to electronic surveillance. More surveillance does not solve problems such as terrorism, but rather brings about a climate of permanent suspicion where citizens are always automatically suspect of being criminals. It is short-sighted and a technological-deterministic attitude to think that more surveillance technology brings about more security and peace. Law and order politics are superficial measures that ignore the underlying socio-economic and political causes of societal problems. Corporations have an economic interest in surveillance. If they gather data on consumers/users, they can sell these data to advertising clients. As long as there is capitalism, there will be media corporations (such as studiVZ, Facebook, MySpace, and others) that sell their audience as commodity to advertising clients because they are necessarily driven by the logic of profitability. It is not an accident that corporations like studiVZ, Facebook, or MySpace have introduced advertising options such as personalized advertising that are based on the surveillance of profiles and usage behaviour. It is also not an accident that one has to opt out of such features, and not has to opt in. Economic surveillance is profitable, therefore media

³⁶ "PLATTERWATCH dokumentiert den Aufbau des Überwachungsstaats und den Abbau des Rechtsstaats. Wir sammeln Facts vom Trojaner und vom IMSI-Catcher bis zur amerikanischen Homeland Security mitten in Österreich. PLATTERWATCH begleitet den Innenminister: mit Fotoapparat und Kamera, quer durch Österreich. Wir stellen den Minister online" (<http://www.platterwatch.at>, accessed on December 8, 2008).

corporations and other firms engage in it. It is unlikely that they will automatically limit these endeavours because their primary interest is and must be the accumulation of money profits. Therefore opting out of existing advertising options is not a solution to the problem of economic and political surveillance. Even if users opt out, media corporations will continue to collect and assess certain data, to sell the users as audience commodity to advertising clients, and to give personal data to the police. Citizen action can limit surveillance actions of corporations, but it will not secure citizens from corporate and state surveillance because the underlying problems are dominant corporate interests and the existence of new imperialism (Harvey 2003, Panitch/Leys 2004, Wood 2003). Surveillance on social networking sites should therefore be framed in the context of pressing political problems, such as global war and the unequal distribution of wealth and income. To try to advance critical awareness and to surveil corporate and political surveillers are important political moves for guaranteeing civil rights, but they will ultimately fail if they do not recognize that electronic surveillance is not a technological issue that can be solved by technological means or by different individual behaviours, but only by bringing about changes of society.

Neo-Luddite solutions to electronic surveillance, i.e. to stop using the Internet or social networking sites, would not be a wise move because the data in our survey indicate that young people find making and maintaining contacts and friendships with the help of the Internet a tremendous opportunity that they consider very important. 59.1% see maintaining existing contacts and 29.8% establishing new contacts as major advantage of social networking sites. Neo-Luddism would create a group of critical Internet dropouts that would not only be disconnected from the Internet, but also disconnected from social opportunities that bring advantages. Neo-Luddism would therefore question electronic surveillance, but at the same time intensify the digital divide. It would bring disadvantages such as meeting less people and staying less in contact with family members, old friends, colleagues, etc.

One alternative is to create non-commercial, non-profit social networking platforms on the Internet. It is not impossible to create successful non-profit Internet platforms, as the example of Wikipedia, which is advertising-free, has free access, and is financed by donations, shows. But the difficulty is that social networking platforms have to store large amount of data, especially profile data that contain images, videos, etc, which requires tremendous server capacities. It is certainly easier and probably more efficient to organize such huge data storage endeavours in the form of profit-oriented businesses. But this orientation at the same time brings about the risk of extended and intensified electronic surveillance. We are not saying that non-commercial, non-profit platforms are devoid of this risk, but that there is a reduced likelihood that electronic surveillance for economic reasons will take place on such platforms and an increased likelihood that such platforms will try to protect its users from state surveillance. Within capitalism, it is certainly very difficult to try to organize such non-profit online alternatives because everything that is non-profit and non-commercial tends to be confronted by shortages of resources, which makes sustainable performance difficult. Trying to organize alternatives might be precarious, difficult, and confronted with a high probability of potential failure. But the same time it might be the only constructive alternative to corporate control and corporate concentration processes in the Internet economy that tend to reinforce processes of economic and political electronic

surveillance.

There are many remaining research questions that can be tasks for future research. The study at hand focused on the relationship of surveillance and the use of social networking sites by students in Salzburg, Austria. Such studies could also be undertaken beyond the local context, for example at the national or the European level. Also comparative studies between different localities, nations, cultures, and continents would be interesting. The study at hand was focused at students. Students are certainly early adopters of new technologies and therefore of primary interest for social research because their technology usage might anticipate larger societal trends. But nonetheless it is also important to study the use of new technologies by other groups that are frequently more disadvantaged in technology use than students and therefore confronted with additional problems. Therefore another potential task for future research is to study the relationship of surveillance and social networking sites for whole populations and for groups other than students.

9. Summary

9.1. Theoretical Foundations

There is a large interest in integrated social networking sites (ISNS) in the global Internet public. ISNS have become popular with the emergence of web 2.0 and web 3.0. Web 1.0 is a computer-based networked system of human cognition, web 2.0 a computer-based networked system of human communication, web 3.0 a computer-based networked system of human co-operation. Online platforms such as MySpace or Facebook – which are the two most well known – are web-based platforms of communication and community-building, i.e. web 2.0 and 3.0 systems. What makes them distinct is that they are integrated platforms that combine many media and information and communication technologies, such as webpage, webmail, digital image, digital video, discussion group, guest book, connection list, or search engine. We find it therefore more appropriate to speak of integrated social networking sites (ISNS) than of social network(ing) sites. ISNS are web-based platforms that integrate different media, information and communication technologies, that allow at least the generation of profiles that display information that describes the users, the display of connections (connection list), the establishment of connections between users that are displayed on their connection lists, and the communication between users. ISNS are just like all computer technologies web 1.0 systems because they reflect and display dominant collective values of society that become objectified and are confronting users. They are web 2.0 technologies because they are used for communication and establishing connections in the form of connection lists. ISNS are web 3.0 technologies because they allow the establishment of new friendships, communities, and the maintenance of existing friendships.

One can distinguish three different approaches of research about ISNS:

1. Techno-pessimistic ISNS research
2. Techno-optimistic ISNS research
3. Critical ISNS research

Techno-pessimistic ISNS research approaches conclude that ISNS are dangerous and pose primarily threats for the users, especially kids, adolescents, and more generally young people. One can also characterize this approach as victimization discourse. Techno-optimistic research about ISNS is a discourse of empowerment. It stresses the potential of technology for autonomy, personal development, freedom, the formation, maintenance, and deepening of communities, love, or friendships. This discourse assesses ISNS fairly positive, it mainly sees advantages, and considers disadvantages as ideological constructs or as minor issues. Critical ISNS research argues that the techno-pessimistic and the techno-optimistic approach do not focus on how ISNS are conditioned by the totality of society. Critical approaches analyze how ISNS usage is conditioned by the capitalist economy, the political system, and dominant cultural value patterns and conflicts.

Electronic surveillance by nation states and corporations aims at controlling the behaviour of individuals and groups, i.e. they should be forced to behave or not behave in certain ways because they know that their appearance, movements, location, or ideas are or could be watched by electronic systems. After September 11, 2001,

electronic surveillance has been intensified. The European Commission passed the Data Retention Directive (2006/24/EC) on March 15, 2006, which requires all member states to pass laws that guarantee that information and communication service providers store source, destination, and other data on a communication for at least 6 months. In December 2007, the Social Democratic Party of Austria (SPÖ) and the Austrian Peoples Party (ÖVP) changed the Security Police Act (Sicherheitspolizeigesetz) so that all information and communication providers are required to pass on personal data of users, if the police ask for it.

There are two major influences on the character of contemporary surveillance society: a political and an economic one. On the one hand, new imperialism has produced a situation, in which war and terror potentially reinforce each other, and the West reacts by increasing surveillance. This results in a contradiction between freedom and security and the short-sighted belief that more surveillance solves societal problems. On the other hand, not only the state, but also corporations have an interest in gathering personal data in order to develop personalized advertising strategies that target individual tastes and related tastes by aggregating and assessing user data.

studiVZ, MySpace, and Facebook are the platforms that our study focused on.

When registering, users must agree that studiVZ can store their usage behaviour, can send them emails and messages about news that concern studiVZ, can send up to five advertisement emails and messages per month to them, and that profile information is analyzed for providing personalized advertisements. The latter three points can be deactivated once one is registered by changing the privacy settings. This is an opt-out and not an opt-in-process. The privacy policy of studiVZ states that users agree that usage data are saved for a maximum of six months. The users also agree that this data and their clickstream are analyzed for being provided with personalized advertisements. Users can opt out of personalized advertisements. Profile data can be used for personalized advertisements. There is an opt-out from this option. The users agree to receive advertising and technical messages per mail and message service, unless s/he opts out. The users agree that their data are provided to the police if this is necessary for public safety or law enforcement.

By signing up to Facebook, users agree to its terms of use and thereby grant the company a license for using and selling all content that is uploaded to the platform. Facebook stores personal data and usage data. These data are also used for personalized services. Facebook automatically uses targeted advertising. Facebook is allowed to automatically collect information on users from other websites and to publish these data on the users' Facebook profiles. Facebook is allowed to share user data with its advertising clients. It may pass on data to authorities for crime prevention or law enforcement.

MySpace allows targeted personalized advertising that is automatically activated. Users can opt out, but doing so is very difficult. There is no menu setting in the privacy options that allows doing so, only a link in the privacy policy that users have to follow. Third party advertisers are allowed to collect information from profiles. Users can opt out, but again doing so is very complicated and only possible by following a link in the privacy policy. MySpace may share personal information, such as email addresses, with

advertising clients for “business reasons”. This means that in such cases companies are allowed to send advertising messages per email to MySpace users. MySpace is allowed to disclose personal information of its users to law enforcement agencies.

9.2. Research Method

We conducted an empirical case study on the relationship of surveillance society and ISNS usage by students in Salzburg. The research was carried out from October to December 2008. The questionnaire was available for 50 days to the students. We constructed a questionnaire that consisted of 35 (single and multiple) choice questions and 3 open-ended questions, and 5 interval-scaled questions. The questionnaire was implemented as an electronic survey with the help of the online tool Survey Monkey.

702 respondents participated in the survey. 28 datasets were deleted from the dataset because the respondents indicated that they were no students or former students and the study focuses on academic usage of ISNS. The remaining N=674 datasets were analyzed

Most of the respondents are heavy users of integrated social networking sites (ISNS). 39.3% use such platforms several times per day, 22.8% once a day (figure 10). So 62.1% of the respondents use ISNS at least once a day.

52.3% of the respondents read the terms of use of ISNS in detail or almost entirely, 47.7% read them only partly, superficial, or never. This shows that information behaviour concerning interest in what Internet companies are allowed to do with user data is almost equally split between a group that rather cares and a group that rather not cares.

9.3. Surveillance Knowledge and Critique of Surveillance

A surveillance knowledge index was calculated by combining the answers to several questions that tested this knowledge. 16.5% (0 correct answers) of the respondents have no, 65.3% (1 correct answer) little, 16.5% (2 correct answers) average, and 1.8% (3 correct answers) high knowledge of surveillance. The median of the surveillance knowledge index is 1 (little knowledge of surveillance).

Bivariate correlations between the surveillance knowledge index and other factors show that the surveillance knowledge index is significantly (at the 0.01 level) negatively correlated to female gender (positively to male gender) and the white-collar status of a student’s father. It is significantly (at the 0.01 level) positively correlated to the status of a student’s father as househusband, income, and the size of the location that the students have been living in for most of their lifetime. The analysis shows overall that gender and class and the urban/rural-differential are three factors that influence surveillance knowledge.

We combined the answers to five scaled questions to an overall index (surveillance critique index). The statistical average of this index is 17.3 (scale: 0-25, 0=no critique towards surveillance, 25=high level of critique towards surveillance) (N=613). This indicates a rather critical stance of the students in our sample towards surveillance.

67.4% of the respondents are critical or rather critical of surveillance (N=613).

Bivariate correlations show that the surveillance critique index is significantly (at the 0.01 level) negatively correlated to female gender (positively to male gender), studying natural sciences, and the usage frequency of ISNS. It is significantly (at the 0.01 level) positively correlated to the number of semesters studied, studying social sciences, and income. In our study, gender, the type and extension of higher education, class, and usage frequency of social networking sites are factors that influence the degree of critical consciousness on surveillance.

How can it be explained that there seems to be little knowledge of actual surveillance, but a high level of criticism towards surveillance? There seems to be a general feeling of students that surveillance is dangerous, threatens the privacy of all individuals, and creates a climate, in which one is automatically considered to be a potential criminal or terrorist. So young people seem to be socialized in a way that tends to create suspicion towards surveillance. For example many pupils in school read and discuss books like George Orwell's "1984" and Aldous Huxley's "Brave New World". But there is not much knowledge about the actual laws in Europe and Austria that regulate surveillance. So for example the amendment of §53 of the Austrian Security Police Act (Sicherheitspolizeigesetz) at the end of 2007 and the European Data Retention Directive are hardly known. Our interpretation is that Austrian institutions (such as the educational system, schools, universities, politicians and the political system, or the media) provide young people with the impression that surveillance as such is dangerous, but that it is not something one has to worry about in Austria. The amendment of the Security Police Act was passed on December 6, 2007. It brought about more surveillance rights for the police in Austria. From November 22 until December 20, 2007, a total of only 23 articles that dealt primarily with the amendment of the security police act were published in 8 Austrian newspapers. This is an indication that a lack of information and of public discussion could be one of the reasons why the students in our survey tend to be rather critical of surveillance, but tend to have little knowledge of the actual judicial situation of surveillance in Austria and Europe.

9.4. studiVZ

88.3% of our respondents are studiVZ users. This confirms the fact that studiVZ is the most used ISNS in Austria and Germany. 91.8% of the studiVZ users answered correctly that studiVZ gathers and stores data about their usage behaviour. 85.6% of the studiVZ users know that studiVZ does not reuse and resell personal data of users. These two results show that students in Salzburg have a relatively good knowledge of what studiVZ is allowed and not allowed to do with their data. 46.6% of the studiVZ users have read the new terms of use that were introduced at the beginning of 2008, whereas 41.8% have not read them. This is a relatively balanced distribution. For the majority of users (55.2%), trust into studiVZ has remained the same after the new terms of use took effect. For a small minority, trust has increased (6.1%), for 38.7% it has decreased. 75.0% of the studiVZ users have deactivated to receive messages from studiVZ advertising clients per email or the studiVZ message service. 58.04% have deactivated receiving personalized advertisements. 69.1% have deactivated the option that studiVZ can send them announcements on new features (figure 24). Combining these three information behaviours by adding one point for each deactivation, we calculated the

studiVZ information behaviour index. In total, 49.2% have opted out of all three advertising options and 20.5% have opted out of two advertising options. 7.8% have opted out from only one advertising option and 22.6% have not opted out of any advertising option. After the new terms of use came into effect, the standard advertising settings for all old and new users were that advertising clients of studiVZ are allowed to send ads to users per email and the studiVZ message service, that personalized advertising is enabled, and that studiVZ can send announcements to users.

These results show that students in Salzburg who use studiVZ tend to have good knowledge of what studiVZ is allowed to do with their data and tend to have taken steps for guaranteeing that advertising and personalized advertising are minimized. Bivariate correlations show that the knowledge users have about what studiVZ is allowed to do with their personal data is positively correlated with the surveillance critique index at a significance level of 0.01. Bivariate correlations also show that users tend to deactivate the possibilities that studiVZ has for sending them advertisements or personalized advertisements, if they tend to read terms of use in general and if they are critical of surveillance. Although students tend to rather not read terms of use and privacy policies of social networking sites in general, in the case of the new terms of use of studiVZ that were introduced at the beginning of 2008, 46.6% of the studiVZ users said that they had read the terms in detail before agreeing and 38.7% say that their trust in studiVZ decreased after the new terms had come into effect.

Information about the changes in privacy, surveillance, and advertising that studiVZ planned by introducing new terms of use, seems to have activated the critical potential of the students that is present in the form of a general critical attitude towards surveillance so that a majority of students have actively taken steps to limit the amount and type of advertising they receive.

The change of the terms of use was also reported by the mass media. A comparison of newspaper and magazine articles on the issue shows that most of them straightforwardly announced that the change of the terms of use means more surveillance and less privacy in order to maximize economic profits of the Holtzbrinck corporation. This coverage seems to have positively influenced students' knowledge about studiVZ and the resulting information behaviour. But besides news coverage on the new studiVZ terms of use, there was also an online campaign. This campaign was mainly an information campaign and not a manifestation of electronic civil disobedience. Our survey data indicate that the online information campaign succeeded in drawing attention to the issue of surveillance by studiVZ and let a vast majority of users to disable advertising options. Nonetheless personalized advertising and advertising messages per email and message service have been introduced and are now standard settings on studiVZ. The studiVZ information campaign did not attract a very large number of active users and seems not to have reached a co-operative level of protest, but it seems to have succeeded in bringing many users to deactivate advertising options. But of course advertising and targeted advertising continue to exist on studiVZ, which means that the platform sells its users as an audience commodity to advertising clients in order to accumulate money capital.

Overall, media information and an online information campaign seem to be some of the causes of the high degree of knowledge and the high degree of critical information

behaviour of the students in our sample in respect to studiVZ.

9.5. Facebook

39.5% of the respondents use Facebook, which is clearly a lower number than in the case of Facebook (88.3%). 94.0% of the Facebook users in our survey answered correctly that Facebook is allowed to collect and store data on their information behaviour. Only 20.4% knew that Facebook is allowed to reuse and resell personal data. 54.5% knew that advertising clients of Facebook are allowed to gather data on the information behaviour of users. Only 33.2% answered correctly that Facebook is always allowed to send them personalized advertising. By combining the answers to these four questions, we collected the Facebook knowledge index: 4.7% of the Facebook users had little knowledge about Facebook (no correct answer), 31.5% small knowledge (one correct answer), 29.8% average knowledge (two correct answers), 26.0% good knowledge (three correct answers), and 8.1 a high degree of knowledge (four correct answers). This means that only 34.1% of the Facebook users had a good or high degree of knowledge on what Facebook is allowed to do with their data, whereas in the case of studiVZ users the degree of correct answers to such questions was on average 88.7% (the average of 91.8% and 85.6%). The knowledge on what platforms are allowed to do with personal data is much higher in the case of studiVZ than in the case of Facebook. An explanation for this difference can be that studiVZ is more discussed between friends, more discussed in the media, and had attracted the attention of many users when it changed its terms of use, whereas Facebook is less known and less discussed in personal conversations and in the public.

68.4% of the Facebook users in our survey have activated social advertisements on Facebook (social ads is a kind of personalized advertising that calculates ads based on friendship groups). 59.9% have activated Facebook beacon, which collects onsite and offsite usage data and publishes these on users' newsfeeds. On studiVZ, on average 67.4% of the users in our survey have opted out of advertising options, whereas on Facebook on average only 35.9% of the users opted out of these options. This shows that critical information behaviour is higher on studiVZ than on Facebook. An explanation for this difference is that studiVZ is more known, more widely used, more discussed in personal conversations and in the public, and has attracted the attention of users and the public when it changed its terms of use.

68.4% of the Facebook users in our survey have activated social advertisements on Facebook (social ads are a kind of personalized advertising that calculates ads based on friendship groups). 59.9% have activated Facebook beacon, which collects onsite and offsite usage data and publishes these on users' newsfeeds. On studiVZ, on average 67.4% of the users in our survey have opted out of advertising options, whereas on Facebook on average only 35.9% of the users opted out of these options. This shows that critical information behaviour is higher on studiVZ than on Facebook. An explanation for this difference is that studiVZ is more known, more widely used, more discussed in personal conversations and in the public, and has attracted the attention of users and the public when it changed its terms of use.

Bivariate correlations show that there is a significant positive correlation between the surveillance critique index and the surveillance knowledge index on the one hand and

the Facebook knowledge index on the other hand. This result confirms that the surveillance parameters have an influence on the usage of ISNS. But nonetheless critical information behaviour on Facebook and knowledge about Facebook are rather small because Facebook is not so much known, and not so much discussed in personal conversations and in the public. Therefore the influence of the surveillance parameters remains limited.

9.6. MySpace

15.9% of the respondents in our survey use MySpace. This is a much lower number than in the case of studivZ (88.3%) and a lower number than in the case of Facebook (39.5%). We combined the answers to four questions that tested the users' knowledge about what MySpace is allowed to do with their data in order to calculate the MySpace Knowledge Index. 15.8% of the MySpace users in our survey have high knowledge of MySpace, 34.7% have good knowledge of MySpace, 43.2% have average knowledge of MySpace, 6.3% have small knowledge of MySpace, and 0% have no knowledge of MySpace. So 50.5% of the MySpace users in our survey have high or good knowledge of MySpace, whereas the remaining 49.5% have average, little, or no knowledge of the platform. In the case of Facebook, 34.1% of the users have a good or high degree of knowledge about what Facebook is allowed to do with their data, whereas in the case of studivZ users, the degree of correct answers to such questions was on average 88.7% (the average of 91.8% and 85.6%). The data show that there is a large difference between the knowledge that users have on studivZ and the knowledge that they have about MySpace and Facebook. That users know so much about studivZ and not so much about MySpace and Facebook can best be explained by the fact that there is more private and public debate about studivZ because it is the most used ISNS in Austria and Germany and by the negative media coverage and the online information campaign that emerged when studivZ changed its terms of use at the beginning of 2008 so that more surveillance and less privacy became possible.

85.2% of the MySpace users in our survey have activated personalized advertising (figure 35), 69.7% allow all advertising companies to send them ad messages (figure 36). This means that on average 22.6% opted out of advertising options on MySpace. In comparison, on average 67.4% of the users in our survey have opted out of advertising options on studivZ and on average 35.9% of the users opted out of these options on Facebook. That users are much more critical towards advertising on studivZ than on MySpace and Facebook can be explained by the fact that the advertising and economic surveillance practices of studivZ have been a public and interpersonal topic that affected studivZ's image negatively, when the platform changed its terms of use at the beginning of 2008. MySpace and Facebook are much less used, known, and discussed in Austria and Germany than in other countries like the USA or the United Kingdom.

We asked the respondents what they think the greatest advantages and disadvantages, i.e. opportunities and risks, of social networking sites were with the help of two open questions.

9.7. Advantages and Disadvantages

Maintaining existing friendships, family contacts, etc. with the help of social networking sites is the most important advantages that the students in our survey mention. 59.1% of them consider it as a major advantage. 29.8% say that establishing new contacts is very important, 19.9% mention finding and renewing old contacts and friendships as major advantage. Maintaining existing contacts seems to be more important than establishing new contacts or renewing old contacts on social networking sites.

55.7% of the respondents say that political, economic, or personal surveillance as a result of data abuse, data forwarding, or a lack of data protection is a main threat of social networking sites. 23.1% say it is problematic that personal affairs that should better be kept private and should not be known by others tend to become public on social networking sites.

Although students are very well aware of the surveillance threat, they are willing to take this risk because they consider communicative opportunities as very important. That they expose themselves to this risk is caused by a lack of alternative platforms that have a strongly reduced surveillance risk and operate on a non-profit and non-commercial basis.

9.8. Usage in Comparison

There is a large concentration of users on studiVZ (88.3% of the respondents), which implies that there is also a market concentration with one dominant actor. Other important platforms are Facebook (39.5%), MySpace (15.9%), Xing (9.0%), Lokalisten (7.4%), and Szene1 (4.3%). The remaining 61 platforms that were mentioned in our survey, each reach less than 1% of the respondents. This means that among the 67 platforms listed by the respondents, we find one large platform, 5 medium-sized ones, and 61 small ones. These data give reason to assume that profit distribution in the social networking market is highly centralized.

9.9. Implications and Conclusions

Our first recommendation is that critical educators, critical scholars, social movements, consumer groups, data protection specialists/groups, consumer protection specialists/groups, critical citizens' initiatives, unions, critical media, critical politicians, and political parties that are critical of surveillance present the topic of the surveillance society on a very concrete level that shows how citizens are immediately affected by surveillance by engaging in activities such as using the Internet, using social networking sites, using mobile phones, leaving data traces in everyday life, etc.

The most successful strategy for strengthening public discourse on an issue is to try to organize campaigns that tackle political issues and show how citizens are immediately negatively affected by certain political conditions. Public campaigns can certainly have limits, especially if there are dominant institutions and actors that have opposing views and have strong influence on the media and public discourse by political and economic power. Therefore one should not be overoptimistic concerning the

possibilities and perspectives for organizing critical discourse in a society that is economically and politically stratified, i.e. shaped by economic and political power differentials. Nonetheless, the only way to bring about change is to try to organize collective articulations of discontent with certain situations.

Our second recommendation is that critical citizens, critical citizens' initiatives, consumer groups, social movement groups, critical scholars, unions, data protection specialists/groups, consumer protection specialists/groups, critical politicians, critical political parties observe closely the relationship of surveillance and corporations and document instances where corporations and politicians take measures that threaten privacy or increase the surveillance of citizens. Such documentation is most effective if it is easily accessible to the public. The Internet provides means for documenting such behaviour. It can help to watch the watchers and to raise public awareness. In recent years, corporate watchdog organizations that run online watch platforms have emerged. There are limitations to such projects, such as resource precariousness and an antagonism between resource precariousness and political autonomy.

There are no easy solutions to the problem of civil rights limitations due to electronic surveillance. Opting out of existing advertising options is not a solution to the problem of economic and political surveillance. Even if users opt out, media corporations will continue to collect and assess certain data on them, to sell the users as audience commodity to advertising clients, and to give personal data to the police. To try to advance critical awareness and to surveil corporate and political surveillers are important political moves for guaranteeing civil rights, but they will ultimately fail if they do not recognize that electronic surveillance is not a technological issue that can be solved by technological means or by different individual behaviours, but only by bringing about changes of society. Therefore our fourth recommendation is to situate the topic of electronic surveillance in the context of larger societal problems in public discourse.

Our fifth recommendation is to create non-commercial, non-profit social networking platforms on the Internet. It is not impossible to create successful non-profit Internet platforms, as the example of Wikipedia, which is advertising-free, has free access, and is financed by donations, shows. But the difficulty is that social networking platforms have to store large amount of data, especially profile data that contain images, videos, etc, which requires tremendous server capacities. It is certainly easier and probably more efficient to organize such huge data storage endeavours in the form of profit-oriented businesses. But this orientation at the same time brings about the risk of extended and intensified electronic surveillance. We are not saying that non-commercial, non-profit platforms are devoid of this risk, but that there is a reduced likelihood that electronic surveillance for economic reasons will take place on such platforms and an increased likelihood that such platforms will try to protect its users from state surveillance. Within capitalism, it is certainly very difficult to try to organize such non-profit online alternatives because everything that is non-profit and non-commercial tends to be confronted by shortages of resources, which makes sustainable performance difficult. Trying to organize alternatives might be precarious, difficult, and confronted with a high probability of potential failure. But the same time it might be the only constructive alternative to corporate control and corporate concentration processes in the Internet economy that tend to reinforce processes of economic and

political electronic surveillance.

10. References

- Acquisti, Alessandro and Ralph Gross. 2006. *Imagined communities: Awareness, information sharing, and privacy on the Facebook*. In *Proceedings of 6th Workshop on Privacy Enhancing Technologies*, ed. by Phillippe Golle and George Danezis, 36-58. Cambridge, UK: Robinson College.
- Albrechtslund, Anders. (2008). Online Social Networking as Participatory Surveillance. *First Monday* 13 (3).
- Alby, Tom. 2007. *Web 2.0. Konzepte, Anwendungen, Technologien*. München: Hanser.
- Baker, James R. and Susan M. Moore. 2008. Distress, coping, and blogging: Comparing new Myspace users by their intention to blog. *CyberPsychology & Behavior* 11 (1): 81-85.
- Ball, Kirstie S, and Frank Webster, eds. 2003. *The intensification of surveillance. Crime, terrorism and warfare in the information age*. London: Pluto Press.
- Barabási, Albert-László. 2003. *Linked*. New York: Plume.
- Barnes, Susan. (2006). A privacy paradox: Social networking in the United States. *First Monday* 11 (9).
- Baym, Nancy. 2007. The new shape of online community: The example of Swedish independent music fandom. *First Monday* 12 (8).
- Beer, David. 2006. The pop-pickers have picked decentralised media: The fall of top of the pops and the rise of the second media age. *Sociological Research Online* 11 (3).
- Beer, David. 2008a. Making friends with Jarvis Cocker: Music culture in the context of Web 2.0. *Cultural Sociology* 2 (2): 222-241.
- Beer, David. 2008b. 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.
- Bernardo, Theresa A. 2007. Harnessing collective knowledge to create global public goods for education and health. *Journal of Veterinary Medical Education* 34 (3): 330-334.
- Bogard, William. 2006. Surveillance Assemblages and Lines of Flight. In *Theorizing Surveillance*, edited by David Lyon, 97-122. Cullompton: Willan.
- boyd, danah. 2004. Friendster and publicly articulated social networks. In *Proceedings of ACM Conference on Human Factors in Computing Systems*, 1279-1282. New York: ACM Press.
- boyd, danah. 2005. *Why web 2.0 matters: Preparing for glocalization*. http://www.zephoria.org/thoughts/archives/2005/09/05/why_web20_matte.html (Accessed on July 9, 2007).
- boyd, danah 2006a. Friends, Friendsters, and MySpace Top 8: Writing community into being on social network sites. *First Monday* 11 (12).
- boyd, danah. 2006b. *Identity production in a networked culture: Why youth heart MySpace*. Talk at AAAS 2006 (part of panel: "It's 10PM: Do You Know Where Your Children Are ... Online!"). St. Louis, Missouri: February 19, 2006.
- boyd, danah. 2007a. The significance of social software. In *BlogTalks reloaded*, edited by Thomas N. Burg, 15-30. Norderstedt: Books on Demand.
- boyd, danah. 2007b. Viewing American class divisions through Facebook and MySpace. *Apophenia Blog Essay*. June 24. <http://www.danah.org/papers/essays/ClassDivisions.html>
- boyd, danah. 2008a. Facebook's privacy trainwreck. *Convergence* 14 (1): 13-20.
- boyd, danah. 2008b. Why youth (heart) social network sites: The role of networked

- publics in teenage social life. In *Youth, identity, and digital media*, ed. David Buckenham, 119-142. Cambridge, MA: MIT Press.
- boyd, danah and Nicole B. Ellison. 2007. Social networking sites: definition, history, and scholarship. *Journal of Computer-Mediated Communication* 13 (1).
- boyd, danah and Jeffrey Heer. 2006. Profiles as conversation: Networked identity performance on Friendster. In *Proceedings of Thirty-Ninth Hawai'i International Conference on System Sciences*. Los Alamitos, CA: IEEE Press.
- Bruns, Axel 2007. Prodisage, generation C, and their effects on the democratic process. In *Proceedings of the conference: Media in transition 5, MIT, Boston*. <http://web.mit.edu/comm-forum/mit5/papers/Bruns.pdf> (Accessed on October 28, 2008)
- Burg, Thomas N. 2003. MonsterMedia. Monstrosity in the face of weblogs. In *BlogTalks*, edited by Thomas N. Burg, 83-100. Norderstedt: Books on Demand.
- Byrne, Dara N. 2007. Public discourse, community concerns, and civic engagement: Exploring Black Social Networking Traditions on BlackPlanet.com. *Journal of Computer-Mediated Communication* 13 (1).
- Cain, Jeff. 2008. Online social networking issues within academia and pharmacy education. *American Journal of Pharmaceutical Education* 72 (1).
- Carroll, Kevin S. 2008. Puerto Rican language use on MySpace.com. *Centro Journal* 20 (1): 96-111.
- Charnigo, Laurie and Barnett-Ellis, Paula. 2007. Checking out Facebook.com: The impact of a digital trend on academic libraries. *Information Technology and Libraries* 28 (1): 23-34.
- Coates, Tom. 2005. *An addendum to a definition of social software*. http://www.plasticbag.org/archives/2005/01/an_addendum_to_a_definition_of_social_software/ (Accessed on July 9, 2007).
- Cohen, Nicole S. and Leslie Regan Shade. 2008. Gendering Facebook: Privacy and commodification. *Feminist Media Studies* 8 (2): 210-214.
- Di Gennaro, Corinna and William H. Dutton. 2007. Reconfiguring friendships: Social relationships and the Internet. *Information, Communication & Society* 10 (5): 591-618.
- Donath, Judith and boyd, danah. 2004. Public displays of connection. *BT Technology Journal* 22 (4): 71-82.
- Dourish, Paul. 2001. *Where the action is*. Boston, MA: MIT Press.
- Dringenberg, Rainer. 2002. Auf dem Weg zur Internetgesellschaft - Markierungen und Perspektiven einer Soziologie des Internet. In *Internet – vorgeführt und diskutiert*, edited by Rainer Dringenberg, 96-144. Bochum: EFH RWL Bochum.
- Durkheim, Emile. 1982. *Rules of sociological method*. New York: Free Press.
- Dwyer, Catherine. 2007. Digital relationships in the 'MySpace' generation: Results from a qualitative study. In *Proceedings of the 40th Hawaii International Conference on System Sciences*. Los Alamitos, CA: IEEE Press.
- Dwyer, Catherine, Starr Roxanne Hiltz and Katia Passerini. 2007. Trust and privacy concern within social networking sites. A comparison of Facebook and MySpace. In *Proceedings of the 13th Americas Conference on Information Systems*. Redhook, NY: Curran.
- Ellison, Nicole, 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).
- Ferdig, Richard E., Kara Dawson, Erik W. Black, Nicole M. Paradise Black and Lindsay

- A. Thompson. 2008. Medical students' and residents' use of online social networking tools: Implications for teaching professionalism in medical education. *First Monday* 13 (9).
- Fischer, Tim E. 2006. *Unternehmenskommunikation und Neue Medien*. Wiesbaden: Deutscher Universitäts-Verlag.
- Foucault, Michel. 1977. *Discipline and punish*. New York: Vintage.
- Fuchs, Christian. 2008. *Internet and society: Social theory in the information age*. New York: Routledge. [see also: <http://fuchs.icts.sbg.ac.at/i&s.html>]
- Fuchs, Christian. 2009. Social software and web 2.0: Their sociological foundations and implications. In *Handbook on Web 2.0, 3.0 and X.0: Technologies, business, and social applications*, ed. San Murugesan. Hershey, PA: IGI Global.
- Fuchs, Christian, Wolfgang Hofkirchner, Matthias Schafranek, Celina Raffl, Marisol Sandoval and Robert Bichler. 2008. The evolution of the web. From web 1.0 towards web 2.0 and web 3.0. *International Journal of Internet Science* 3 (1).
- Gandy, Oscar H. 1982. *Beyond agenda setting: Information subsidies and public policy*. Norwood, NJ: Ablex.
- Giddens, Anthony. 1981. *A contemporary critique of Historical Materialism. Vol. 1: Power, property and the state*. London: Macmillan.
- Giddens, Anthony. 1985. *A contemporary critique of Historical Materialism. Vol. 2: The nation-state and violence*. Cambridge: Polity Press.
- Gillmor, Dan. 2006. *We the media. Grassroots journalism by the people, for the people*. Beijing: O'Reilly.
- Goodings, Lewis, Abigail Locke and Steven D. Brown. 2007. Social networking technology: Place and identity in mediated communities. *Journal of Community & Applied Social Psychology* 17 (6): 463-476.
- Graham, Philip. 2000. Hypercapitalism: A political economy of informational idealism. *New Media & Society* 2(2): 131-156
- Gras, Marianne L. 2004. The legal regulation of CCTV in Europe. *Surveillance & Society* 2 (2/3): 216-229.
- Gray, Mitchell. 2003. Urban surveillance and panopticism: Will we recognize the facial recognition society? *Surveillance & Society* 1 (3): 314-330.
- Gross, Ralph, Alessandro Acquisti, and A. & Heinz, H. John III. 2005. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on privacy in the electronic society*, 71-80. New York: ACM Press.
- Gueorguieva, Vassia. 2008. Voters, MySpace, and YouTube. *Social Science Computer Review* 26 (3): 288-300.
- Haddon, Leslie and Shin Dong Kim. 2007. Mobile phones and web-based social networking - Emerging practices in Korea with Cyworld. *Journal of the Communications Network* 6 (January-March 2007): 5-12.
- Haggerty, Kevin D. 2006. Tear down the walls: On demolishing the panopticon. In *Theorizing surveillance*, edited by David Lyon, 23-45. Cullompton: Willan.
- Haggerty, Kevin D. and Richard V. Ericson. 2000. The Surveillant assemblage. *British Journal of Sociology* 51 (4): 605-622.
- Hardt, Hanno. 1992. *Critical communication studies*. New York: Routledge.
- Hargittai, Eszter. 2007. Whose space? Differences among users and non-users of social network sites. *Journal of Computer Mediated Communication* 13 (1).
- Harris, Andrew/Lessick, Susan. 2007. Libraries get personal: Facebook applications, Google gadgets, and MySpace profiles. *Library Hi Tech News* 24 (8): 30-32.
- Harvey, David. 2003. *The new imperialism*. Oxford: Oxford University Press.

- Herring, Susan C., John C. Paolillo, Irine Ramos-Vielba, Inna Kouper, Elijah Wright, Sharon Stoerger, Lois Ann Scheidt and Benjamin Clark. 2007. Language networks on LiveJournal. In *Proceedings of the 40th Hawaii International Conference on System Sciences*. Los Alamitos, CA: IEEE Press.
- Hinduja, Sameer and Justin W. Patchin. 2008. Personal information of adolescents on the Internet: A quantitative content analysis of MySpace. *Journal of Adolescence* 31 (1): 125-146.
- Horkheimer, Max. 1974/2004. *Eclipse of reason*. New York: Continuum.
- Humphreys, Lee. 2007. Mobile social networks and social practice: a case study of Dodgeball. *Journal of Computer Mediated Communication* 13 (1).
- Jones, Harvey and José Hiram Soltren: 2005. *Facebook: Threats to privacy*. Cambridge, MA: MIT. <http://swiss.csail.mit.edu/6095/student-papers/fall05-papers/facebook.pdf>
- Jones, Steve, Sarah Millermaier, Mariana Goya-Martinez and Jessica Schuler. 2008. Whose space is MySpace? A content analysis of MySpace profiles. *First Monday* 13 (9).
- Kellner, Douglas. 1995. *Cultural studies, identity and politics between the modern and the postmodern*. New York: Routledge.
- Kellner, Douglas M. and Meenakshi Gigi Durham. 2006. Adventures in media and cultural studies: Introducing the KeyWorks. In *Media and cultural studies: KeyWorks*, ed. Meenakshi Gigi Durham and Douglas M. Kellner, ix-xxxviii. Malden, MA: Blackwell.
- Kidd, Michael R. 2008. Personal electronic health records: MySpace or HealthSpace. *British Medical Journal* 7652: 1029-1030.
- Kim, Kyung-Hee and Haejin Yun. 2007. Crying for me, crying for us: relational dialectics in a Korean social network site. *Journal of Computer Mediated Communication* 13 (1).
- Knoche, Manfred. 2005. Kommunikationswissenschaftliche Medienökonomie als Kritik der Politischen Ökonomie der Medien. In *Internationale partizipatorische Kommunikationspolitik*, ed. Petra Ahrweiler and Barbara Thomaß, 101-109. Münster: LIT.
- Kolbitsch, Josef and Hermann Maurer. 2006. The transformation of the Web: How emerging communities shape the information we consume. *Journal of Universal Computer Science* 12 (2): 187-213.
- Koskela, Hille. 2006. 'The other side of surveillance': Webcams, power and agency. In *Theorizing surveillance*, edited by David Lyon, 163-181. Cullompton: Willan.
- Krippendorff, Klaus. 2004. Content analysis. An introduction to its methodology. London: Sage. 2nd edition.
- Lampe, Cliff, Nicole Ellison, and Charles Steinfield. 2006a. A Face(book) in the crowd: Social searching vs. social browsing, In *Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work*, 167-170. New York: ACM Press.
- Lampe, Cliff, Nicole Ellison, and Charles Steinfield. 2006b. A familiar Face(book): profile elements as signals in an online social network. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 435-444. New York: ACM Press,
- Lange, Patricia. 2007. Publicly private and privately public: social networking on YouTube. *Journal of Computer Mediated Communication* 13 (1).
- Lenhart, Amanda and Mary Madden. 2007. Social networking websites and teens: an overview. http://www.pewinternet.org/pdfs/PIP_SNS_Data_Memo_Jan_2007.pdf

- (accessed on October 7, 2008).
- 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.
- Liu, Hugo (2007) Social network profiles as taste performances. *Journal of Computer Mediated Communication* 13 (1).
- Liu, Hugo, Pattie Maes and Glorianna Davenport. 2006. Unravelling the taste fabric of social networks. *International Journal on Semantic Web and Information Systems* 2 (1): 42-71.
- 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*. Cambridge: Polity Press.
- Lyon, David. 2001. *Surveillance society. Monitoring everyday life*. Buckingham: Open University Press.
- Lyon, David. 2003. *Surveillance after September 11*. Cambridge: Polity Press.
- Magnuson, Melissa Joy and Lauren Dundes. 2008. Gender differences in "social portraits" reflected in MySpace profiles. *Cyberpsychology & Behavior* 11 (2): 239-241.
- Marcuse, Herbert. 1937/1988. Philosophy and critical theory. In *Negations: Essays in critical theory*, 134-158. London: Free Association.
- Marcuse, Herbert. 1969. *An essay on liberation*. Boston: Beacon Press.
- Marwick, Alice. 2008. To catch a predator? The MySpace moral panic. *First Monday* 13 (6).
- Marx, Karl. 1858/1993. *Grundrisse*. London: Penguin.
- Marx, Karl. 1867/1990. *Capital Volume I*. London: Penguin.
- Marx, Karl. 1885/1992. *Capital Volume II*. London: Penguin.
- Marx, Karl and Friedrich Engels. MEW. *Werke*. Berlin: Dietz.
- Mazer, Joseph, Richard Murphy, Richard and Cheri Simonds. 2007. I'll see you on "Facebook": The effects of computer-mediated teacher self-disclosure on student motivation, affective learning, and classroom climate. *Communication Education* 56 (1): 1-17.
- McCaughey, Martha and Michael D. Ayers, eds. 2003. *Cyberactivism*. New York: Routledge.
- McGee, James B. and Michael Begg. 2008. What medical educators need to know about "Web 2.0". *Medical Teacher* 30 (2): 164-169.
- Meadows-Klue, Danny. 2008. Falling in Love 2.0: Relationship marketing for the Facebook generation. *Direct, Data and Digital Marketing Practice* 9 (3): 245-250.
- Miller, Paul. 2005. *Web 2.0: Building the New Library*. In *Ariadne* 45: <http://www.ariadne.ac.uk/issue45/miller/> (Accessed on July 9, 2007)
- Mitchell, Eleanor and Sarah Barbara Watstein. 2007. The places where students and scholars work, collaborate, share and plan: Endless possibilities for us! *Reference Services Review* 35 (4): 521-524.
- Moreno, Megan A., Norman C. Fost and Dimitri A. Christakis. 2008. Research ethics in the MySpace era. *Pediatrics* 121 (1): 157-161.
- OECD. 2007. Participative Web and user-created content: Web 2.0, wikis and social networking. *SourceOECD* 15 (2007): i-128.
- Ogura, Toshimaru. 2006. Electronic government and surveillance-oriented society. In

- Theorizing surveillance*, edited by David Lyon, 270-295. Cullompton: Willan.
- O'Reilly, Tim. 2005a. *What is Web 2.0?*
<http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html?page=1> (Accessed on July 9, 2007).
- O'Reilly, Tim. 2005b. *Web 2.0: Compact definition*.
http://radar.oreilly.com/archives/2005/10/web_20_compact_definition.html
(Accessed on July 9, 2007).
- Panitch, Leo and Colin Leys ed. 2004. *The new imperialist challenge: Socialist Register 2004: The new imperial challenge*. New York: Monthly Review Press.
- Pascu, Corina, David Osimo, Martin Ulbrich, Geomina Turlea and Jean-Claude Burgelman. 2007. The potential disruptive impact of Internet 2 based technologies. In *First Monday* 12 (3).
- Raacke, John and Jennifer Bonds-Raacke. 2008. MySpace and Facebook: Applying the uses and gratifications theory to exploring friend-networking sites. *Cyberpsychology & Behavior* 11 (2): 169-174.
- Rheingold, Howard. 2000. *The virtual community*. Cambridge, MA: MIT Press.
- Rost, Martin. 1997. Anmerkungen zu einer Soziologie des Internet. In *Soziologie des Internet. Handeln im elektronischen Web-Werk*, edited by Lorenz Gräf and Markus Krajewski, 14-38. Frankfurt am Main: Campus.
- Saveri, Andrea, Howard Rheingold and Kathi Vian. 2005. *Technologies of cooperation*. Palo Alto, CA: Institute for the Future.
- Shirky, Clay. 2003. *Social Software and the politics of groups*.
http://shirky.com/writings/group_politics.html (Accessed on July 9, 2007).
- Smythe, Dallas W. 1981/2006. On the audience commodity and its work. In Meenakshi G. Durham and Douglas M. Kellner (Eds.) *Media and cultural studies*, 230-256. Malden, MA: Blackwell.
- Stefanac, Suzanne. 2007. *Dispatches from blogistan. A travel guide for the modern blogger*. Berkeley, CA: New Riders.
- Stutzman, Frederic. 2006. An evaluation of identity-sharing behavior in social network communities. *iDMAa Journal* 3 (1).
- Swisher, Peter Simeon. 2007. The managed web: A look at the impact of web 2.0 on media asset management for the enterprise. In *Journal of Digital Asset Management* 3 (1): 32-42.
- Tapscott, Don and Anthony D. Williams. 2006. *Wikinomics: How Mass Collaboration Changes Everything*. London: Penguin.
- Thelwall, Mike. 2008. Social networks, gender, and friending. *Journal of the American Society for Information Science and Technology* 59 (8): 1321-1330.
- Thompson, Lindsay A, Kara Dawson, Richard Ferdig, Erik Black, J. Boyer, Jade Coutts and Nicole Paradise Black. 2008. The intersection of online social networking with medical professionalism. *Journal of General Internal Medicine* 23 (7): 954-957.
- Toffler, Alvin. 1980. *The third wave*. New York: Bentam.
- Tom Tong, Stephanie, Brandon Van Der Heide, Lindsey Langwell, and Joseph B. Walther. 2008. Too much of a good thing? The relationship between number of friends and interpersonal impressions on Facebook. *Journal of Computer-Mediated Communication* 13 (3).
- Tönnies, Ferdinand. 1988. *Community & society*. New Brunswick, NJ: Transaction Books.
- Tufekci, Zeynep. 2008a. Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology and Society* 28 (1): 20-

36.

- Tufekci, Zeynep. 2008b. Grooming, Gossip, Facebook and Myspace. *Information, Communication & Society* 11 (4): 544-564.
- Valkenburg, Patti M., Jochen Peter and Alexander P. Schouten. 2006. Friend networking sites and their relationship to adolescents' well-being and social self-esteem. *Cyberpsychology & Behavior* 9 (5): 584-590.
- Van de Donk, Wim, Brian Loader, Paul Nixon, and Dieter Rucht, eds. 2004. *Cyberprotest*. New York: Routledge.
- Walther, Joseph B., Brandon Van Der Heide, Sang-Yeon Kim, David Westerman and Stephanie Tom Tong. 2008. The role of friends' appearance and behavior on evaluations of individuals on Facebook: are we known by the company we keep? *Human Communication Research* 34 (1): 28-49.
- Wasserman, Stanley and Katherine Faust, Katherine. 1997. *Social network analysis*. Cambridge: Cambridge University Press.
- Webb, Matt. 2004. *On social software consultancy*. http://interconnected.org/home/2004/04/28/on_social_software (Accessed on July 9, 2007).
- Webb, Maureen. 2007. *Illusions of security: Global surveillance and democracy in the post-9/11 world*. San Francisco: City Lights.
- Weber, Max. 1968. *Economy and society: An outline of interpretive sociology*. New York: Bedminster Press.
- Webster, William R. 2004. The diffusion, regulation and governance of CCTV in the UK. *Surveillance & Society* 2 (2/3): 230-250.
- Winner, Langdon. 1980/1999. Do artifacts have politics? In *The social shaping of technology*, ed. Donald MacKenzie and Judy Wajcman, 28-40. Maidenhead: Open University Press.
- Winter, Rainer. 2004. Cultural Studies. In *A companion to qualitative research*, ed. Uwe Flick, Ernst von Kardoff and Ines Steinke, 118-122. London: Sage.
- Wood, Ellen Meiksins. 2003. *Empire of Capital*. London: Verso.
- Wright, Steve. 2005. The ECHELON trail: An illegal vision. *Surveillance & Society* 3 (2/3): 198-215.
- Ybarra, Michele L. and Kimberly J. Mitchell. 2008. Distress, coping, and blogging: Comparing new Myspace users by their intention to blog. *Pediatrics* 121 (2): E350-E357.
- Zhao, Shanyang, Sherri Grasmuck and Jason Martin. 2008. Identity construction on Facebook: Digital empowerment in anchored relationships. *Computers in Human Behavior* 24 (5): 1816-1836.
- 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): 1-34.

Annex A: Survey Questionnaire

The Usage of Social Networking Platforms by Students in Salzburg

The ICT&S Center of the University of Salzburg conducts a study of students' usage behaviour of social networking platforms (studiVZ, MySpace, Facebook, etc) in Salzburg.

We appreciate if you can help is in this research by filling out a questionnaire.

Completing the survey will take approximately 15 minutes. All data is treated confidentially and anonymously.

The survey is open for completion from October 13 until November 30, 2008.

We will give away three Amazon vouchers (60 €, 25 €, 25 €) in a lottery among the participants. Supplying your email-address is voluntary and the address will be stored independently of your survey data.

It would be of great help to us, if you inform your friends in Salzburg, who also use StudiVZ, about this survey. The more fully completed questionnaires we receive, the better results we will obtain.

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

Contact:

PD Dr. Christian Fuchs
ICT&S Center
Universität Salzburg
Sigmund Haffner Gasse 18
5020 Salzburg
christian.fuchs@sbg.ac.at
Phone 0662-8044-4823

General Questions

(1)

Are you?

Male

Female

(2)

How old are you?

(3)

Are you:

A bachelor student

A master student

A doctoral student

A research associate

University administration

I am no student and do not work at university

I am a former student

(4)

If you are a student, in which semester do you study currently?

(5)

If you have studied or are studying: Which kind of programme did you or are you attending?

- Humanities or Social Sciences
- Natural Sciences
- Engineering Sciences
- Arts
- Sports
- Medicine
- Law

(6)

What is your average monthly income (including subsidies you receive by your parents and by the state)?

- Less than 400 Euro
- 401-600 Euro
- 601-800 Euro
- 801-1000 Euro
- 1001-1200 Euro
- 1201-1500 Euro
- More than 1500 Euro

(7)

Where have you lived for the largest part of your life?

- A village (< 5 000 inhabitants)
- A small town (5 000-20 000 inhabitants)
- A medium-sized city (20 000-100 000 inhabitants)
- A large town (100 000 – 1 000 000 inhabitants)
- A metropolis (> 1 000 000 inhabitants)

(8)

What is the highest educational achievement in your family (mother, father)?

- Compulsory school
- School leaving examination (Matura)
- University graduation
- Doctoral degree

(9)

What is the occupation status of your father?

- Blue-collar worker
- White-collar employee
- Civil servant
- Self-employed, entrepreneur
- Retiree
- Unemployed
- Househusband

(10)

What is the occupation status of your mother?

- Blue-collar worker
- White-collar employee
- Civil servant
- Self-employed, entrepreneur
- Retiree
- Unemployed
- Housewife

General Questions on Social Networking Platforms

(11)

How often do you visit social networking platforms as studiVZ, Facebook, MySpace, etc?

- Several times a day
- Once a day
- Several times a week
- Once a week
- Several times a month
- Once a month
- Never

(12)

Which of the following social networking platforms do you use (multiple answers)?

- StudiVZ
- Facebook
- MySpace
- Others (please indicate): _____

(13)

When I register at or use a platform, then I read the terms of use and the privacy policy:

- No, never.
- Superficially or hardly.
- Partly.
- Almost completely.
- Always in detail.

Open-ended Questions

(14)

What are in your opinion the greatest advantages of social networking platforms as studiVZ, Facebook, MySpace, etc?

(15)

What is your greatest concern about social networking platforms as studiVZ, Facebook, MySpace, etc?

(16)

Other comments that you want to make on social networking platforms?

Surveillance

What is the correct answer?

(17)

Web platforms in Austria have to pass on personal data (name, email-address, etc) to the police:

Yes, always if the police demand it. X

No, never

Only if the police have a juridical order that was passed by a court and is handed over to the provider.

(18)

Platforms such as studiVZ, Facebook or MySpace store data about me only as long as I do not delete my account.

Yes, this is correct.

No, this is incorrect X.

(19)

I can describe in one sentence exactly what the Data Retention Directive is:

Yes

No

The following questions are answered with the help of a scale

1 ----- 2----- 3----- 4----- 5----- 6

I completely disagree I fully agree.

(20) If you have nothing illegal to hide, then you need not be afraid of surveillance.

(21) I trust that social networking platforms such as studiVZ, MySpace, or Facebook deal in a responsible way with my data.

(22) In Austria, there are only few laws that allow the surveillance of Internet and phone communication. Citizens are therefore well protected from state surveillance.

(23) Firms have a strong interest in gathering personal data of Internet users.

(24) State surveillance of citizens has increased after the terrorist attacks in New York on September 11, 2001.

Questions about studiVZ

Please answer spontaneously.

(25) Is the following statement correct? studiVZ gathers and stores data on my usage behaviour on the platform (visited pages, time of log in, sending of messages and entries, membership in groups, etc).

Yes X

No

(26) Is the following statement correct? studiVZ is allowed to reuse and sell my user-

generated content (photos, videos, etc).

- Yes
- No X

(27) studiVZ has changed its terms of use and privacy policy at the beginning of 2008. All users had to agree if they wanted to continue using the platform. Select the option below that most closely describes your response when asked to agree to the new privacy terms.

- I agreed to the new terms without reading them in detail.
- I have read the new terms thoroughly before I agreed.
- I have registered to studiVZ during the year 2008 and therefore have never been confronted by the old terms.
- I have terminated my usage of studiVZ.
- I have first terminated my usage of studiVZ, but then again started to use it.

(28) How did the change in policy effect how you think about studiVZ:

- I feel more comfortable about my privacy due to the change in the privacy policy
- I am more concerned about my privacy due to the change in the privacy policy
- Nothing has changed about the feeling that I have about privacy protection on studiVZ

We now ask you to log into your studiVZ profile, to take a look at your privacy settings, and, without making changes, to let us honestly know your settings. You find your privacy settings in the left-hand column of the screen ("privacy", subcategories "my privacy" and "advertising settings")

Bearbeiten Darstellung Verlauf Lesezeichen Fenster Hilfe

studiVZ | Meine Privatsphäre

http://www.studivz.net/Terms/Options

Metcon Metro Club ... apartments View Property Condos & To... Oodle.com Furl It Philadelphia...ennsylvania 1600-1

STUDIVERZEICHNIS suche einladen hilfe kartext boutique einstieg ra

Meine Privatsphäre Plauderkasten

Meine Privatsphäre meinVZ Ignorierte Nutzer Gruppe **Werbe-Einstellungen**

Damit studiVZ weiter kostenlos bleibt, zeigen wir Dir Werbung.

Zum Schutz Deiner Daten verpflichten wir uns zu den folgenden Grundsätzen:

1. studiVZ erhebt, verarbeitet und nutzt Deine personenbezogenen Daten nur unter strengster Einhaltung der Datenschutzgesetze der Bundesrepublik Deutschland.
2. studiVZ wird in keinem Fall Deine personenbezogenen Daten zu Werbe- oder Marketingzwecken Dritten zur Verfügung stellen (z.B. werden Dein Name oder Deine E-Mail-Adresse niemals an Werbepartner weitergeben).
3. Entgegen der üblichen Praxis bei vielen Communities und Personen-Netzwerken schließt studiVZ einen Zugriff Internet-Suchmaschinen und Personen-Suchmaschinen auf Profile oder Beiträge seiner Nutzer explizit aus.

Hier kannst Du jederzeit Einstellungen zur Verwendung Deiner Daten vornehmen. So kannst Du selbst entscheiden, in welcher Form Dir Werbung auf studiVZ angezeigt werden soll.

▼ **Einstellungen über den Erhalt von Informationen über die studiVZ Ltd.**

Hier kannst Du einstellen, ob Du Mitteilungen zu neuen oder verbesserten Funktionen des Netzwerkes, zu Veranstaltungen oder zu speziellen Angeboten der studiVZ Ltd. erhalten möchtest. Diese können über den Nachrichtendienst von studiVZ oder per E-Mail versendet werden.

Botschafter des Tages:
Lieber zu Fuß zum Strand, als mit dem Mercedes zur Arbeit.

(29) Advertising settings:

Have you activated the option that you receive advertisements per email or the studiVZ message service by advertising partners of studiVZ?

Yes, I have activated this option.

No, I have deactivated this option.

(30) I have selected to receive the following type of advertisements:

I receive personalized advertisements, i.e. advertisements that fit my personal interests

I do not receive personalized advertisements, but advertisements that are selected by chance

(31) I have selected the option that studiVZ can send me information about new features, events, or special offers per email or the studiVZ message service

Yes, I have activated this option.

No, I have deactivated this option.

Questions about Facebook

(32) Is the following statement correct? Facebook gathers and stores data on my usage behaviour on the platform (visited pages, time of log in, sending of messages and entries, membership in groups, etc).

Yes X

No

(33) Is the following statement correct? Facebook is allowed to reuse and sell my user-generated content (photos, videos, etc).

Yes X

No

(34) Is the following statement correct? Advertising clients of Facebook are allowed to gather data on my behaviour on the platform (visited pages, membership in groups, etc)

Yes X

No

(35) Facebook allows that I receive targeted personalized advertisements, for which my interests are stored and assessed.

Yes, always. X

No, never.

Only if I agree explicitly.

Yes, but only as long as I agree.

(36) Please take now a look at your privacy settings on Facebook and tell us, without making changes, more about them. You find these settings in the upper right corner under "Settings->Privacy-Settings".

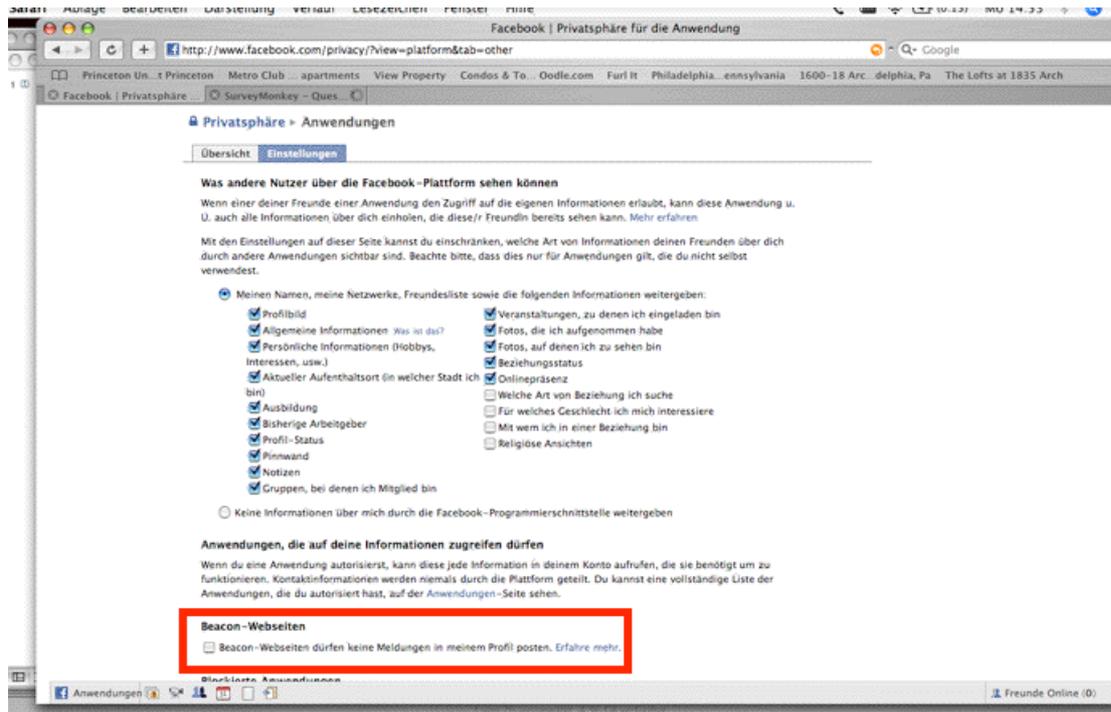


Under "News Feed and Wall"->"Social Ads", the following setting is selected:

- Appearance in Social Ads of only my friends
- Appearance in Social Ads of no one

(37) Now please go to "Privacy->Applications". What are the selected settings concerning "Beacon Websites"

- "Don't allow Beacon websites to post stories to my profile" is deactivated.
- "Don't allow Beacon websites to post stories to my profile" is activated.



Questions about MySpace

(38) Is the following statement correct? MySpace gathers and stores data on my usage behaviour on the platform (visited pages, time of log in, sending of messages and entries, membership in groups, etc).

- Yes X
 No

(39) Is the following statement correct? MySpace is allowed to reuse and sell my user-generated content (photos, videos, etc).

- Yes
 No X

(40) Is the following statement correct? Advertising clients of MySpace are allowed to gather data on my behaviour on the platform (visited pages, membership in groups, etc)

- Yes X
 No

(41) MySpace allows that I receive targeted personalized advertisements, for which my interests are stored and assessed.

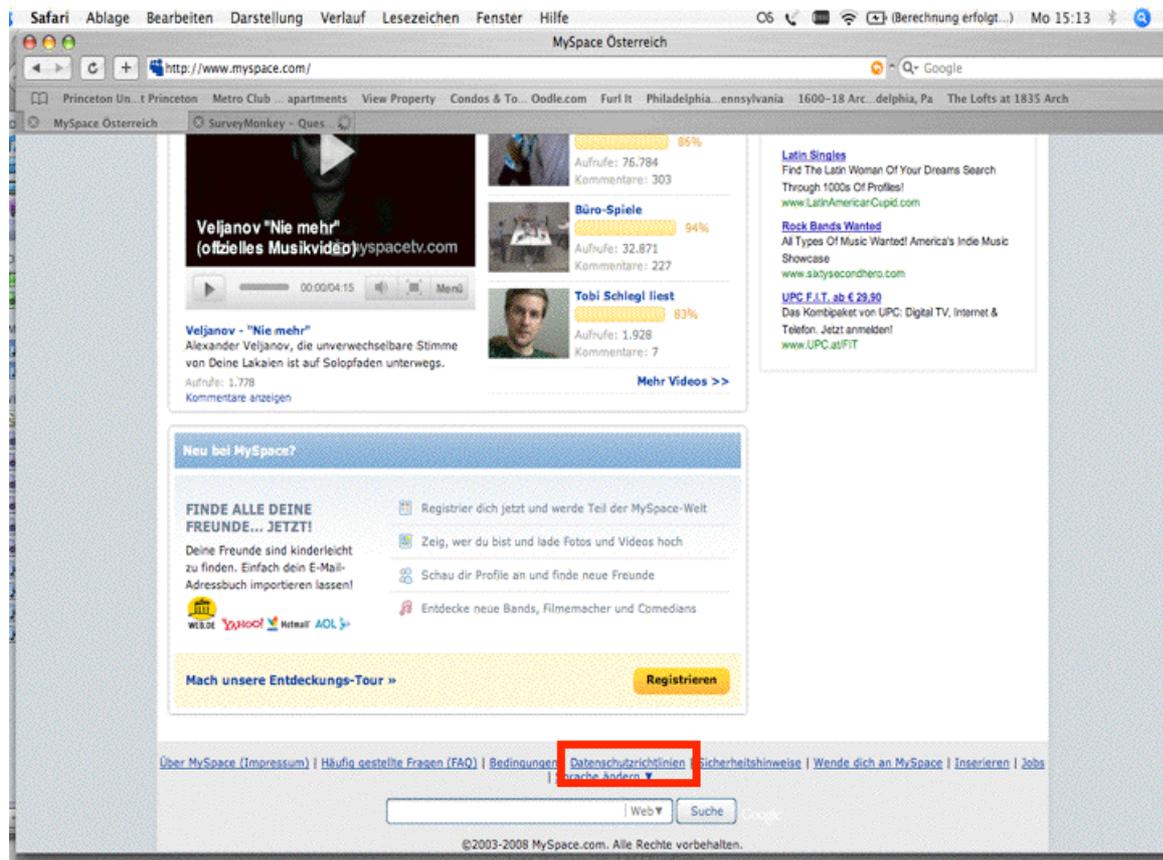
- Yes, always.
 No, never.
 Only if I agree explicitly.
 Yes, but only as long as I agree. X

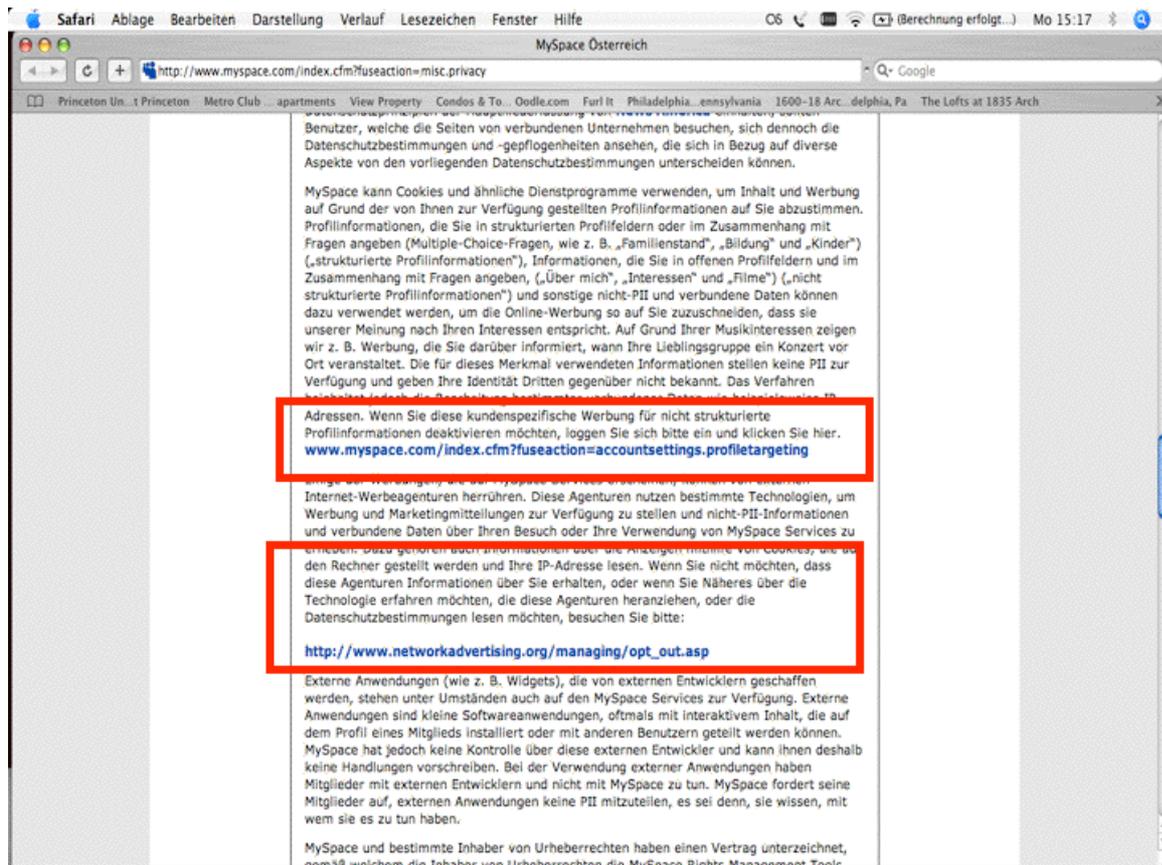
(42) Please log into MySpace and follow the link "Privacy Policy" (in the row at the

bottom of the web page), search for the following text and follow the link in order to see the advertising settings:

“If you would like to disable advertising customization for Non-Structured Profile Information, please log in and click here:

<http://www.myspace.com/index.cfm?fuseaction=accountsettings.profiletargeting>”





After following the link, you see a settings menu. Please do not make any changes and tell us more about your settings. Which option is chosen?

- Display relevant advertisements based on my interests expressed in my profile
- Do not display relevant advertisements; I want to receive non-customized advertising that may not be of interest to me.

(43) Please log into MySpace and follow the link “Privacy Policy” (in the row at the bottom of the web page), search for the following text and follow the link in order to see the advertising settings:

“To opt out of information collection by these companies, or to obtain information about the technologies they use or their own privacy policies, please click here: http://www.networkadvertising.org/managing/opt_out.asp”

You see a settings menu. Please do not make any changes and tell us how many times opting out of a specific advertising network or company is activated:

- No opt-out option is activated
- 1
- 2-5
- 6-10
- 11-15
- All opt-out options are activated

If you want to take part in winning one of 3 Amazon vouchers, then please enter your email address. It will be stored independently of your answers.

If you want to receive updates on research reports that result from this project, then enter your email address.

Participate in the lottery

Receive information on research reports

email address: _____

Thank you for participating in this study. Your answers are important for us in order to advance research about social networking.

The winners of the vouchers are drawn randomly after the survey ends on November 30, 2008. They will be notified per email.

We are happy if you inform your friends in Salzburg that also use social networking platforms about this survey:

<http://www.sbg.at.st>