Ethics Inf Technol (2010) 12:171–185
DOI 10.1007/s10676-010-9220-z

ORIGINAL PAPER

studiVZ: social networking in the surveillance society

Christian Fuchs

Published online: 20 March 2010
© Springer Science+Business Media B.V. 2010

Abstract This paper presents some results of a case study of the usage of the social networking platform studiVZ by students in Salzburg, Austria. The topic is framed by the context of electronic surveillance. An online survey that was based on questionnaire that consisted of 35 (single and multiple) choice questions, 3 open-ended questions, and 5 interval-scaled questions, was carried out ($N = 674$). The knowledge that students have in general was assessed with by calculating a surveillance knowledge index, the critical awareness towards surveillance by calculating a surveillance critique index. Knowledge about studiVZ as well as information behaviour on the platform were analyzed and related to the surveillance parameters. The results show that public information and discussion about surveillance and social networking platforms is important for activating critical information behaviour. In the case of studiVZ, a change of the terms of use in 2008 that brought about the possibility of targeted personalized advertising, was the subject of public discussions that influenced students' knowledge and information behaviour.

Keywords Social networking sites · Surveillance · Privacy · Surveillance society · Web 2.0 · Critical theory · studiVZ · Consumer surveillance · Economic surveillance · Targeted advertising · Capitalism

C. Fuchs (✉)
Unified Theory of Information Research Group, ICT&S Center: Advanced Studies and Research in Information and Communication Technologies & Society, University of Salzburg, Sigmund Haffner Gasse 18, 5020 Salzburg, Austria
e-mail: christian.fuchs@sbg.ac.at

Introduction

Web 2.0 and social networking sites are the subject of everyday coverage in the mass media. So for example the German Bild Zeitung wrote: "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, 2008). Die Zeit wrote: "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).

Such media clippings show that social networking sites (SNS) have become an important topic of public discussions in the German-speaking world. Such mass-mediated debates are frequently oversimplified and one-dimensional (Horkheimer and Adorno 1944; Marcuse 1964), but they nonetheless show that there is a vital interest in how online communication tools transform society and our social relations. Social networking sites are highly frequented websites. In November 2009, Facebook was ranked number 2 in the list of the globally most accessed websites (source: alexa.com, accessed on December 1, 2009). MySpace was ranked number 12 (websites (source: alexa.com, accessed on December 1, 2009). The worldwide popularity of these sites shows that it is important to conduct case studies of SNS usage behaviour.

In September 2008, the SNS studiVZ was with 158 583 022 visits the fourth most frequently visited website in Germany.[1]

[1] Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern, http://www.ivw.eu, accessed on December 10, 2008.

In this paper the results of a study on Austrian students' studiVZ usage in the context of electronic surveillance is presented. The study was conducted in the local context of Salzburg/Austria, and it is subject to the following three research questions:

1. How knowledgeable are students about the rise of a surveillance society?
2. How critical are students of the rise of a surveillance society?
3. How do the degree of knowledge about surveillance and the degree of critical consciousness on surveillance influence the usage of studiVZ?

First, some background on studiVZ and on surveillance in Austria will be given. Then, the research methodology will be explained and the results of the study will be presented and discussed. Finally, some conclusions will be drawn.

Background

Surveillance can be defined as the collection and usage of data on individuals or groups so that control and discipline of behaviour can be exercised by a present threat of being targeted by violence (Fuchs 2008, 267–277). This notion of surveillance can for example be found in the works by Foucault (1979), in neo-Foucauldian surveillance studies, and in the approaches of representatives of the political economy of surveillance such as Gandy (1993) and Ogura (2006). Advertising is a means for advancing capital accumulation and is in critical studies considered as a form of manipulation and therefore as an expression of asymmetric power relations. On the Internet in general, and especially on web 2.0 platforms such as Facebook or MySpace, many personal data are available, which explains the interests of advertising firms to engage in surveillance of these data in order to accumulate capital. Most social networking sites are owned and operated by large corporations. Corporate surveillance is an important field of surveillance studies (for example: Gandy 1993; Ogura 2006). Therefore analyzing economic surveillance in relation to the Internet is an important task for contemporary surveillance studies.

studiVZ (studi = student, VZ = Verzeichnis, list, list of students) is an SNS focusing on students as user group and is primarily used in Germany and Austria. Ehssan Dariani and Dennis Bemmann founded 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, Nature. About 86.6% of the studiVZ users come from Germany, 7.6% from Austria.[2]

studiVZ does neither define property nor usage rights of the content in its terms of use, therefore, the users are the sole owners of all content they post on their profiles. The privacy policy of studiVZ states that users agree to their usage date being saved for a maximum of 6 months (studiVZ privacy policy §4). The users also agree that their profile data and clickstream are analyzed in order to provide them with personalized advertisements (studiVZ privacy policy §§4, 5). They can opt out of personalized advertising (§§4, 5), but such advertisings are set as standard option. The users agree to receive advertising and technical messages per mail and the studiVZ message service, unless they opt out (Privacy policy §6). The users also agree that their data are provided to the police for public safety or law enforcement if necessary (Privacy policy §7). The privacy policy allows to opt out of personalized advertisement and receiving ads per mail and message service, but nevertheless the usage behaviour of all members is stored (§7). 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 was implemented in Germany (studiVZ is a German legal entity) in 2007.

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 all 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) that all information and communication providers are required to pass on users' personal and transmission data if the police ask for it (§53). No judicial order is required. In contrast to Austria, the German Federal Constitutional Court decided in March 2008 that providers must grant the police access to communication data only in case of a judicial order and a severe criminal act.

The Data Retention Directive and the Austrian Security Police Act show that in contemporary societies, surveillance is a central political issue, especially after September 11, 2001. In recent years, these political changes led to an increased academic interest in studying surveillance (e.g. Ball and Webster 2003; Haggerty and Ericson 2000; Lyon 2001, 2003; Webb 2007) that has also been reflected in the

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

launch of the journal *Surveillance & Society* in 2002. As SNS are huge data collections, it is an important research task to analyze SNS usage behaviour in the context of surveillance.

Specific research that has been conducted on SNS includes: 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 et al. 2008), friendship (Boyzd 2006), gender (Magnuson and Dundes 2008; Cohen and Shade 2008), implications for libraries (Charnigo and Barnett-Ellis 2007; Harris et al. 2007), language use (Carroll 2008; Herring et al. 2007), media theory (Beer 2006), medical education (Ferdig et al. 2008; McGee and Begg 2008; Thompson et al. 2008), music culture (Baym 2007; Beer 2008a), pharmacy education (Cain 2008), place and identity (Goodings et al. 2007), psychological distress (Baker and Moore 2008), research ethics (Moreno et al. 2008), self-esteem and sociability (Zywica and Danowski 2008), SNS as virtual learning environments (Mitchell and Watstein 2007) and their role in education (Mazer et al. 2007), studies on 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 2008), the fusion of public and privacy (Lange 2007), the rise of marketing relationships on SNS as a challenge for public relations (Meadows-Klues 2008), and work skills (Bernardo 2007). Surveillance and social networking sites thus far have with some exceptions (e.g. Albrechtslund 2008) been rather unstudied. It is therefore important to conduct concrete studies that cover this topic.

The topic of surveillance and SNS is related to the issue of privacy protection. Most published studies concentrate on privacy aspects of SNS, only single ones on surveillance. Acquisti and Gross (2006) conducted an online survey of SNS users at Carnegie Mellon University ($N = 294$) and found no significant correlation between privacy concerns and information revelation. Much personal information was revealed. Dwyer (2007), based on qualitative interviews ($N = 18$), sees a tradeoff between free access and diminished privacy protection as a cause of information revelation on SNS. Dwyer et al. (2007) conducted an online survey of SNS users and also found high levels of revelation ($N = 117$). Jones et al. (2008) report on a content analysis of MySpace profiles ($N = 1378$) that only a low percentage of users provided personally identifiable data such as full names, their names on Internet messaging services, or their email addresses. 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. Tufekci (2008) ($N = 704$) reports on 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 orientation, 72.2% their sexual orientation, and 75.6% their relationship status. Hinduja and Patchin (2008) conducted a content analysis of MySpace profiles ($N = 9{,}282$) and report that only a small number of users included an email address or other ways to personally contact them. Sonia Livingstone (2008) conducted qualitative interviews with SNS users ($N = 16$, age between 13 and 16) and found out that teenagers typically want to share their profile with friends and keep it private from others. Barnes (2006) speaks of a privacy paradox: Adults are concerned about privacy invasion, whereas teens make personal information public so that it can be analyzed by marketers, schools, government agencies, and online predators. Fogel and Nehmad (2009) found in a survey ($N = 205$) that men are more likely to display their phone number and home addresses on SNS profiles than women. Lewis et al. (2008) conducted an analysis of students' SNS profiles at one university ($N = 1{,}710$). They found out that students with more SNS friends and higher SNS activity are more likely to have private profiles. They also report that the women in their sample are more likely to have private profiles than men. Hodge (2006) argues that courts should take measures so that the fourth amendment does not get lost on SNS. Albrechtslund (2008) introduces the concept of participatory surveillance in respect to SNS.

Most studies that cover the issue of privacy and SNS focus on individual privacy concerns and individual privacy-related behaviour on SNS. The issue of surveillance is more of a macro-topic that requires usage behaviour being framed by societal context variables. These context variables are for example the role that corporations, state legislation, and state institutions play in surveillance. The analysis of surveillance and SNS therefore is in need of a research approach that takes political contexts into account (Beer 2008b). This means that applying a surveillance studies approach to SNS research has to take the issue of corporate surveillance and state surveillance into account. The existing studies show that privacy and surveillance are important topics in SNS research. They also show that there is much more focus on the privacy topic than on surveillance and that the advertising mechanisms used on SNS such as targeted advertising as well as the question of the influence of attitudes on surveillance and privacy on SNS advertising settings, have thus far hardly been studied. This paper contributes to overcoming the predominant individualism of SNS research and to giving more attention to societal issues such as surveillance and how societal phenomena influence SNS.

Tavani (2008) points out that privacy can be seen as a unitary concept standing on its own, as derivative concept derived from other concepts such as property, security, liberty, life, and freedom, or as multifaceted notion. James Moor (2000) speaks in this context of intrinsic and instrumental ways for justifying privacy. One could also speak of intrinsic and extrinsic justifications of privacy. Privacy can be seen either as a right or an interest (Tavani 2008). Tavani identifies four kinds of privacy:

- Privacy as nonintrusion into one's physical space (physical/accessibility privacy)
- Privacy as noninterference into one's choices (decisional privacy)
- Privacy as nonintrusion and noninterference into one's thoughts and personal identity (psychological/mental privacy)
- Privacy as having control over/limiting access to one's personal information (informational privacy)

Ken Gormley (1992: 1337f) distinguishes four types of privacy definitions: 1. privacy as an expression of one's personhood and personality, 2. privacy as autonomy, 3. privacy as the citizens' ability to regulate information about themselves, 4. multidimensional notions of privacy.

I use surveillance as a negative term that denotes the collection (and eventually storage, usage, combination, transfer, diffusion, and assessment) of data about individuals or groups in order to control and discipline their behaviour by the threat of being targeted by violence or to establish or reproduce domination (Fuchs 2008: 269). Surveillance operates with uncertainty, invisibility, and psychological threats. On SNS, the standard privacy settings in general make the user the automatic target of surveillance that is used for economic purposes: personal data and usage behaviour are stored, analyzed, and transmitted to third parties so that the tastes of the users become known to advertising firms that are allowed to target users with personalized advertising. For the users, the surveillance process is invisible and aims at psychological control of their consumption behaviour.

Surveillance is primarily political surveillance that is conducted by state institutions such as the police, secret services, and the military, and economic surveillance that is conducted by corporations. "Global corporations or national governments control significant portions of the surveillance infrastructure" (Phillips 2009: 337). Surveillance is a necessary aspect of domination because dominative societies need to secure the dominance of certain groups and classes with the help of coercive means and (direct and indirect) violence. Corporations are interested in gathering information about their workers and consumers in order to optimize the production process and maximize profits. States are interested in gathering data about their citizens in order to effectively organize bureaucracy and to prevent and investigate crime. Therefore both economic and political surveillance are necessary aspects of modern society. If the categories surveillance and surveillance societies are used in ways that identify positive aspects of surveillance, then the critical power of the notion is forestalled and the actual dangers of surveillance are trivialized.

Privacy is in modern societies an ideal rooted in the Enlightenment. The rise of capitalism resulted in the idea that the private sphere should be separated from the public sphere and not accessible for the public and that therefore autonomy and anonymity of the individual is needed in the private sphere. The rise of the idea of privacy in modern society is connected to the rise of the central ideal of the freedom of private ownership. Private ownership is the idea that humans have the right to own as much wealth as they want, as long as it is inherited or acquired through individual achievements. There is an antagonism between private ownership and social equity in modern society. How much and what exactly a person owns is treated as an aspect of privacy in contemporary society. To keep ownership structures secret is a measure of precaution against the public questioning or the political and individual attack against private ownership. Capitalism requires anonymity and privacy in order to function. But full privacy is also not possible in modern society because strangers enter social relations that require trust or enable exchange. Building trust requires knowing certain data about other persons. It is therefore checked with the help of surveillance procedures if a stranger can be trusted. Corporations have the aim of accumulating ever more capital. That is why they have an interest in knowing as much as possible about their workers (in order to control them) and the interests, tastes, and behaviours of their customers. This results in the surveillance of workers and consumers. "Companies wish to collect data on customers and clients for many reasons. In particular, knowing one's customers can help to provide better products and services, create longer-term relationships and thereby maximise profits in the long run. It thus seems to be in the interest of companies to maximise the amount of data they can collect on customers" (McRobb and Stahl 2007: 237). The ideals of modernity (such as the freedom of ownership) also produce phenomena such as income and wealth inequality, poverty, unemployment, precarious living and precarious working conditions.

These socio-economic differences pose problems for the maintenance of order and private ownership (crime, political protests, violent conflicts) that need to be contained if modernity wants to survive. As a result, state surveillance is a necessary component of modern societies.

The establishment of trust, socio-economic differences, and corporate interests are three qualities of modernity that

necessitate surveillance. Therefore, modernity on the one hand advances the ideal of a right to privacy, but on the other hand it must continuously advance surveillance that threatens to undermine privacy rights. An antagonism between privacy ideals and surveillance is therefore constitutive for capitalism. This connection has been observed by a number of authors in surveillance studies: "A society of strangers is one of immense personal privacy. Surveillance is the cost of that privacy" (Nock 1993: 1) "Surveillance is the paradoxical product of the quest for privacy" (Lyon 2005: 21). "In our nomadic world the society of strangers seeks privacy that actually gives rise to surveillance. Tokens of trust, such as personal identification numbers and barcoded cards, are demanded to demonstrate eligibility or reputation" (Lyon 2005: 27). "The rise of privacy is accompanied by an alarming and perhaps sometimes welcomed rise of surveillance" (Gumpert and Drucker 2000: 172). "The unprecedented growth of surveillance practices and systems during the twentieth century was greeted, among those who cared, by calls for the protection of privacy" (Lyon 2005: 20). "Most notably, the ethical dimensions of liberal philosophical, political, and judicial attitudes toward privacy come into direct conflict with that distinct but nevertheless related intellectual tradition, economic liberalism" (Sewell and Barker 2007: 356).

Social networking sites are primarily operated by corporations. The typical business model is one that gives free access to the users and aims at accumulating profit by selling the users as commodity to advertising clients. Advertising is the central profit generation mechanism of social networking sites. In order to make advertising on these sites attractive to potential and existing clients, social networking sites make use of their primary resource: the personal data and usage behaviour of their users. This data is not only stored, but also combined, assessed, and transferred to advertising clients to enable targeted advertising. Economic surveillance is therefore a necessary aspect of corporate social networking platforms – information gathering, storage, assessment, and transfer mechanism that enable user commodification and capital accumulation (Fuchs 2010). "The more that people rely on the web for their reading and shopping, the more likely it becomes that data about their interests, preferences, and economic behaviour will be captured and made part of personal profiles" (Froomkin 2000: 1486).

The conducted study is also connected to research on public privacy and surveillance awareness and the awareness of consumers about corporate information surveillance. Wang et al. (1998) elaborated a taxonomy for privacy concerns. They identified improper acquisition (access, collection, monitoring), use (analysis, transfer), and storage of data as well as privacy invasion (unwanted solicitation) as reasons for concerns. McRobb and Stahl studied intrinsic and extrinsic justifications for privacy and found that "e-government organisations are more likely to favour an intrinsic foundation for privacy, while e-business organisations are more likely to take an instrumentalist view" (McRobb and Stahl 2007: 245). An intrinsic foundation means that privacy is considered as a value in-itself, whereas extrinsic justifications derive privacy from other moral values. Sheehan (2002) argues that although privacy concerns are in general high, they are rather low in relation to commercial online applications. In this survey of online privacy concerns ($N = 889$) he found that "individuals' orientation to privacy concern may be influenced by their age and their level of education" (Sheehan 2002: 30). O'Neil (2001) analyzed data from two surveys of Internet use in the USA (N1 = 5,022, N2 = 1,482) and found that "education level does not seem to affect a person's degree of concern about online privacy, and those with higher income levels seem to be less concerned about privacy than those with lower income levels. Additionally, women seem to have higher concerns about privacy than men" (O'Neil 2001: 29). Turow et al. (2005) conducted a survey about the knowledge and attitudes of American online shoppers ($N = 1{,}500$). They found that 75% did "not know the correct response—false—to the statement, 'When a website has a privacy policy, it means the site will not share my information with other websites and companies'" (Turow et al. 2005: 3). The authors conclude that American shoppers are "open to financial exploitation by retailers" (Turow et al. 2005: 3). Hoofnagle and King (2008) conducted a survey of the understandings of online privacy of Californian adults ($N = 991$). They found that a relative majority of 47.3% thought (incorrectly) that privacy policies prohibit third-party information sharing, 58.9% knew correctly that a website that has a privacy policy can use personal information for analyzing online activities, and 56.5% thought incorrectly that privacy policies convey the right to access and correct personal information. The authors conclude: "This survey explores the meaning and misunderstandings of the term 'privacy policy' among consumers. We found that many Californian consumers believe that privacy policies guarantee strong privacy rights. The term 'privacy policy' is functioning in consumers' minds as a privacy seal. A majority of Californians believe that privacy policies guarantee the right to require a website to delete personal information upon request, a general right to sue for damages, a right to be informed of security breaches, a right to assistance if identity theft occurs, and a right to access and correct data. In other cases, a majority believes that privacy policies prohibit common business practices, or simply doesn't know the answer to the question. For instance, a majority either doesn't know or believes that privacy policies prohibit third party information sale, affiliate sharing, government

access to personal information, and enhancement. (…) These findings show that Californian consumers overvalue the mere fact that a website has a privacy policy, and assume that websites carrying the label have strong, default rules to protect personal data" (Hoofnagle and King 2008: 25f, 2).

Methodology

We conducted an empirical case study on the relationship of the surveillance society and SNS usage by students in Salzburg. The research was carried out from October to December 2008. The questionnaire consisted of 35 (single and multiple) choice questions, 3 open-ended questions, and 5 interval-scaled questions and was available to the students for 50 days. 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 on 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 a total of 53 discussion groups on studiVZ, Facebook, and MySpace that are concerned with the students' life in Salzburg. We distributed flyers and 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 item of a newsletter to all students of the University of Salzburg on November 18, 2008. As an incentive for their participation, the research team drew three Amazon vouchers (60€, 25€, 25€) among those who completed the survey.

Knowledge of the surveillance society and its policies was measured with the help of an index (surveillance knowledge index) that was calculated based on the answers given to the 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:
O Yes, always if the police demands for it (X)
O No, never
O Only if the police has a juridical order that was passed by court and is handed over to the provider.

(18)
Platforms such as Facebook or MySpace store data about me only as long as I do not delete my profile.
O Yes, this is correct.
O No, this is incorrect (X).

(19)
I can describe in one sentence exactly what the Data Retention Directive is:
O Yes
O No
X…correct answer

The first question tests the students' knowledge of the Austrian Security Police Act (Sicherheitspolzeigesetz). The second question tests their knowledge about data storage. The third question assesses the 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 (Table 1):

The surveillance critique index can be calculated using the following formula:

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

0–5	uncritical of the surveillance society
6–10	hardly critical of the surveillance society

Table 1 Questions underlying the surveillance critique index

	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, and Facebook deal with my data in a responsible way						
(22) In Austria, there are only a few laws that allow surveillance of Internet and phone communication. Citizens are therefore well protected from state surveillance						
(23) Firms have a strong interest in gathering personal data from 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

11–15 modest criticism of the surveillance society
16–20 rather critical of the surveillance society
21–25 critical of the surveillance society

To answer the research questions 3 and 4, the results obtained for the surveillance knowledge index and the surveillance critique index can be used.

For assessing the usage of studiVZ, we asked questions about the students' knowledge of the platform's privacy policy and terms of use as well as the advertising settings on their profiles. For answering our research questions, the surveillance knowledge index and the critique of surveillance index were correlated with the knowledge about privacy policy and terms of use and with the advertising settings. The most important results are presented within the next section. We have obtained many detailed results, but due to limitations of space only selected ones are presented.

Results

A total of 702 respondents participated in the survey. 28 datasets were deleted 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 with the help of SPSS 16.0. There were 67.5% female and 32.5% male respondents. This reflects the overall gender distribution of students in Salzburg very well. 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 2006.[3] 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, which accounted in total for more than 87% of all respondents. Most of the respondents are heavy users of social networking sites (SNS). About 39.3% use such platforms several times per day, 22.8% once a day (Fig. 1). So 62.1% of the respondents use SNS at least once a day. This indicates that these platforms have become very popular in particular among students in Salzburg and in general among Austrian students. Only 3.4% of the respondents never use such platforms, which indicates that students are highly e-literate/e-educated and value online communication. About 49.5% of the respondents read the terms of use of SNS never or superficially; only 13.9% read them almost entirely or completely (Fig. 2). This shows that information behaviour concerning interest in what Internet companies are allowed to do with user data is rather small.

Our respondents had little knowledge of surveillance in Austria and Europe. Only 8.9% knew that web platforms in Austria always have to give personal data to the police if they demand for it, only 15.7% of the respondents said that they knew what data retention (in German: Vorratsdatenspeicherung) is. However, 79.2% of the respondents knew or guessed right that social networking platforms generally store data even after a user deleted some information or the whole profile. This could indicate that Austrian students know more about surveillance if it immediately concerns technologies that they use very frequently than what they know about general policies that set legal conditions for surveillance. 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%

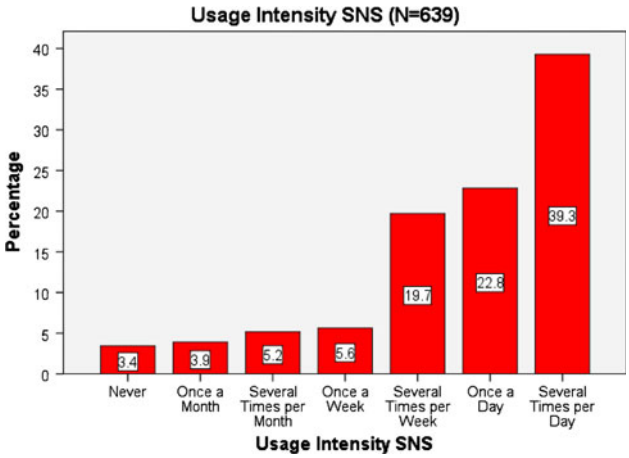

Fig. 1 Usage intensity of SNS by students in Salzburg

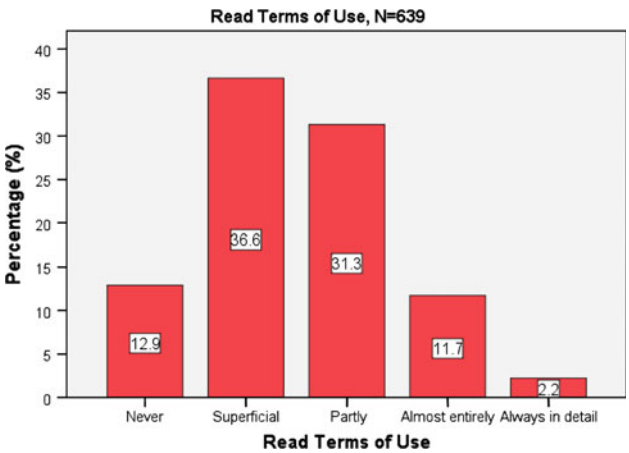

Fig. 2 Salzburg students' intensity of reading the terms of use of SNS

[3] 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.

(2 correct answers) average, and 1.8% (3 correct answers) high knowledge of surveillance (Fig. 3). The median of the surveillance knowledge index is 1 (little knowledge of surveillance).

Five scaled questions 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. For example, 71.8% disagree (to a certain extent) to the statement that one need not be afraid of surveillance if one has nothing to hide. About 53% disagree (to a certain extent) to the statement that social networking platforms can be trusted in how they deal with private data. About 73.2% disagree (to a certain extent) that Austrians are well protected from state surveillance. About 87.0% agree or strongly agree that corporations have great interest in gathering personal data. About 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 over surveillance as a problem. 67.4% of the respondents are critical or rather critical of surveillance ($N = 613$). The exact distribution is shown in Fig. 4.

A total of 88.3% of our respondents use studiVZ, a result that underlines that studiVZ is a frequently used SNS in Austria and Germany. About 91.8% of the studiVZ users answered correctly that studiVZ gathers and stores data about their usage behaviour (Fig. 5). About 85.6% of the studiVZ users know that studiVZ neither reuses nor resells personal data of their users (Fig. 6). 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. About 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 (Fig. 7). 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 (Fig. 8). About 75.0% of the studiVZ users have deactivated the functionality to receive messages from studiVZ advertising clients per email or the studiVZ message service (Fig. 9). About 58.04% have deactivated the functionality to receive personalized advertisements (Fig. 10). About 69.1% have deactivated the option that studiVZ can send them announcements on new features (Fig. 11). Combining these three information behaviours by adding one point for each deactivation, we calculated the studiVZ information behaviour index (Fig. 12). About 22.6% of the studiVZ

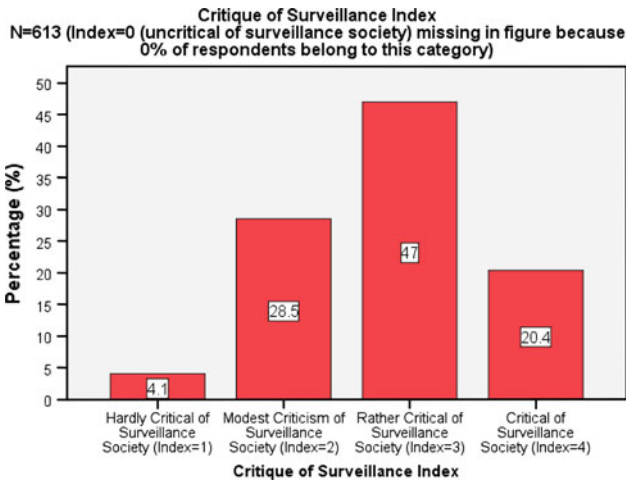

Fig. 4 Surveillance critique index

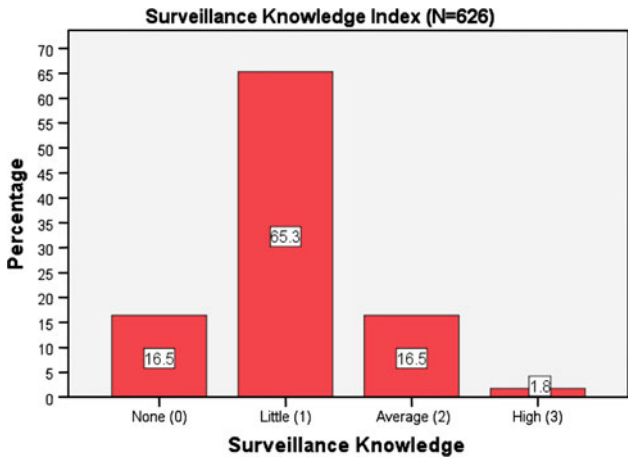

Fig. 3 Surveillance knowledge index

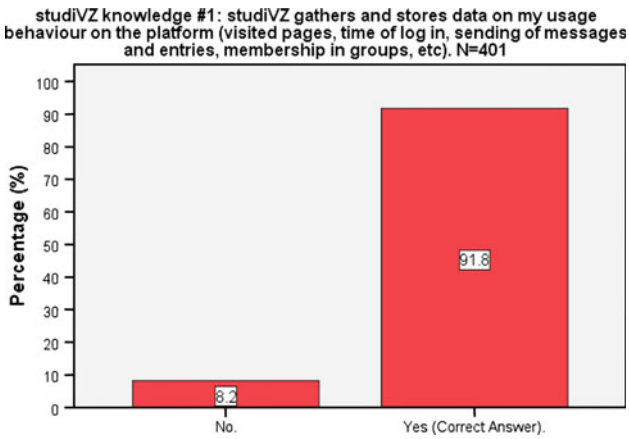

Fig. 5 Knowledge about studiVZ #1

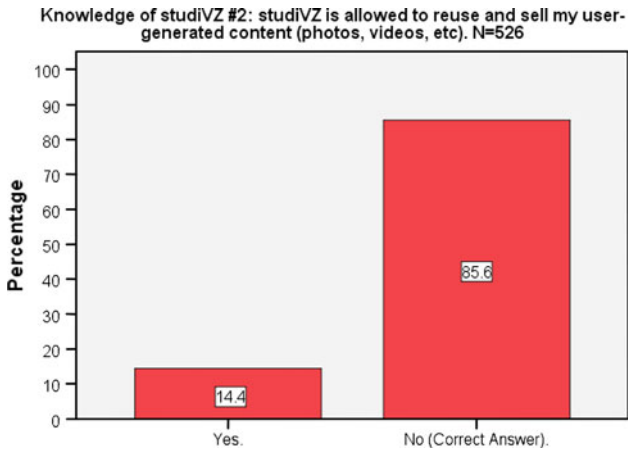

Fig. 6 Knowledge about studiVZ #2

users in our sample are not safe from advertisements, 7.8% have low safety, 20.5% some safety, and 49.2% good safety.

These results show that students in Salzburg using 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.

In Table 2 the results of the 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) are presented. 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

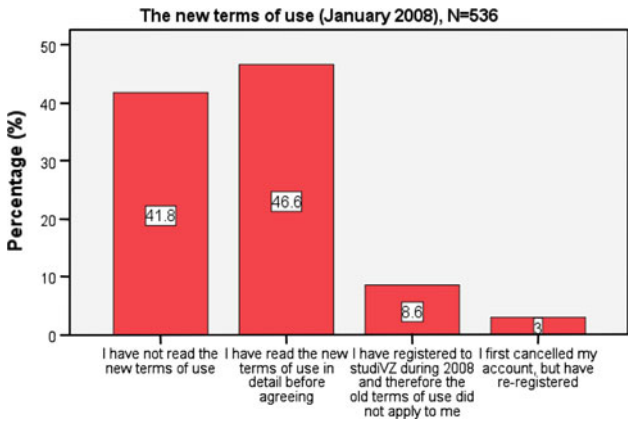

Fig. 7 Behaviour concerning the new terms of use of studiVZ

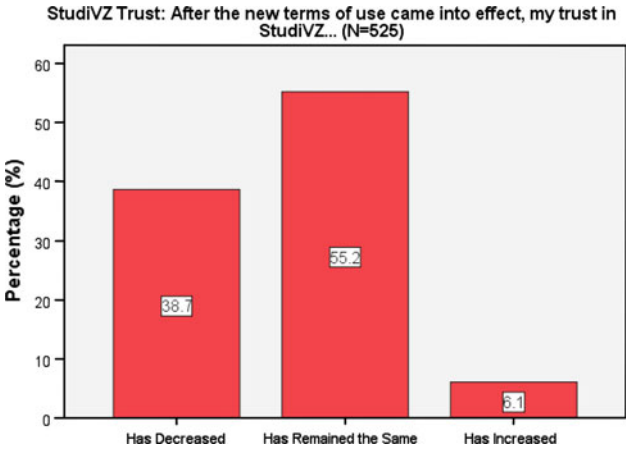

Fig. 8 Trust in studiVZ

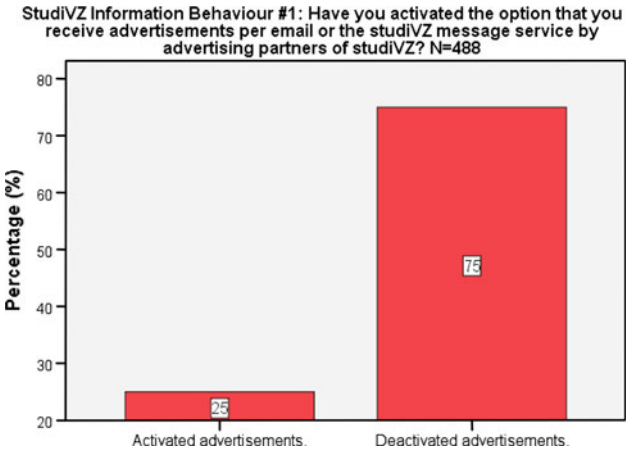

Fig. 9 studiVZ information behaviour #1

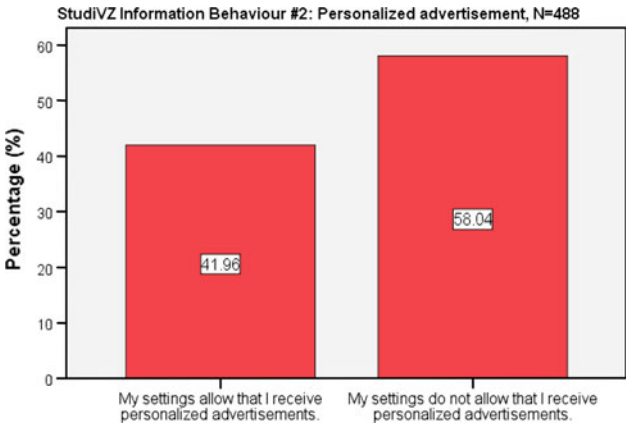

Fig. 10 studiVZ information behaviour #2

surveillance increases the probability that users inform themselves on what studiVZ is allowed to do. Users who read the terms of use of SNS in more detail in general, tend to have read the new terms of use of studiVZ, which is an

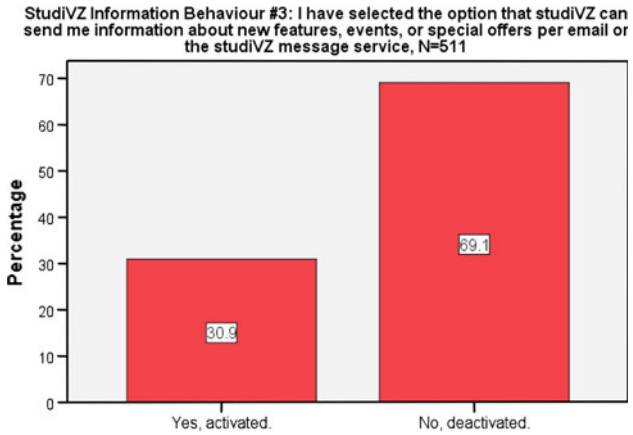

Fig. 11 studiVZ information behaviour #3

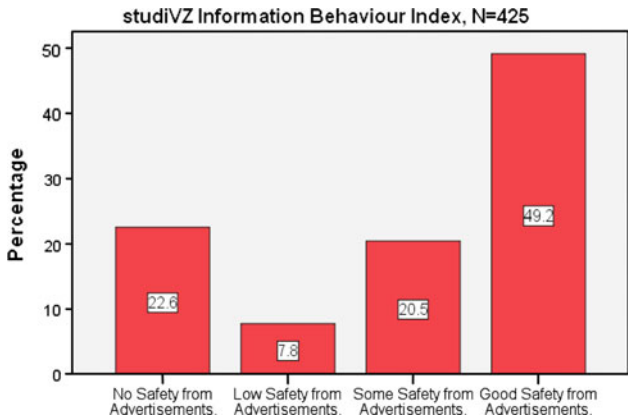

Fig. 12 studiVZ information behaviour index

obvious result. The significant correlation (at the 0.01 significance level) between those two aspects confirms 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 of studiVZ for sending them advertisings or personalized advertisings, if they tend to read terms of use in general and if they are critical of surveillance.

These results will be interpreted in the following.

Discussion

The results of the study show that students in Salzburg using studiVZ have a high knowledge about what the provider is allowed to do with personal data and a high degree of critical information behaviour that led a vast majority of students to opt out of advertising mechanisms if possible. Critical information behaviour involves actions that question the status quo of information systems, it asks if the users really benefit from the standard settings of these systems, and which changes need to be undertaken in order to overcome or lessen power differentials. The correlation analysis showed that especially a general critical attitude towards surveillance has a positive influence on knowledge about studiVZ and critical information behaviour on the platform.

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, 36.6% say they read them only superficially, whereas only 11.7% say they read them almost entirely and 2.2% that they always read them 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 indicates that studiVZ users were suspicious of the new terms being 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 what it is not allowed to do with their personal data. About 91.8% of them know that studiVZ gathers and stores data on their usage behaviour, 85.6% answered correctly that studiVZ is not allowed to reuse or resell user-generated content. This indicates 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 have influenced this high degree of knowledge about studiVZ. After the new terms of use came into effect, the standard advertising settings for all old and new users were set in such way 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 their users. About 75.0% of the studiVZ users in our sample actively opted out of the first advertising option, 58.04% opted out of the second advertising option, and 69.1% opted out of the third advertising option. In total, 49.2% opted out of all three advertising options and 20.5% opted out of two advertising options. About 7.8% opted out from only one advertising option and 22.6% did not opt out of any advertising option at all. These data show that 70% of all

Table 2 Bivariate correlations about studiVZ

	studiVZ knowledge #1	studiVZ knowledge #2	Having read the new terms of use	Trust in studiVZ	studiVZ information behaviour index
Having read the new studiVZ terms of use					
Correlation coefficient				−0.182**	
Sig. (2-tailed)				0.000	
N				386	
Usage intensity SNS:					
Correlation coefficient	0.016	0.112**	0.055	0.082	0.050
Sig. (2-tailed)	0.746	0.010	0.272	0.059	0.304
N	401	526	396	525	425
Read terms of use:					
Correlation coefficient	0.030	0.069	0.358**	−0.181**	0.165**
Sig. (2-tailed)	0.552	0.114	0.000	0.000	0.001
N	401	526	396	525	425
Surveillance critique index:					
Correlation coefficient	0.137**	0.139**	0.093	−0.270**	0.157**
Sig. (2-tailed)	0.006	0.001	0.064	0.000	0.001
N	401	526	396	525	425
Surveillance knowledge index:					
Correlation coefficient	0.081	−0.096	0.092	−0.159**	0.089
Sig. (2-tailed)	0.104	0.028	0.068	0.000	0.066
N	401	526	396	525	425

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

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 the knowledge about studiVZ and critical information behaviour on the studiVZ platform on the other hand. 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 the students have actively taken steps to limit the amount and type of advertising they receive. There seems to be a general critical attitude of the students towards advertising and the usage of personal data and user behaviour by third-party advertising clients.

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 3 shows the five groups with the most members.

In the largest group, information about the changes is provided and there is a call to action for users to disagree ("Appeal to all members: Let your profiles become orphans!", "Apell 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 explains 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 surveillance.

Table 3 studiVZ interest groups on the change of the terms of use with most members (accessed on December 7, 2008)

Group name	Number of members	Number of postings
Achtung–studiVZ ändert die AGB! [Attention—studiVZ changes the terms of use!]	3,820	8,748
Widerspruch gegen die neuen AGB (12/07) [Opposition to the new terms of use (12/07)]	1,620	1,042
"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

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 et al. 2004) and cyberactivism (McCaughey and Ayers 2003) have been coined for describing the organization of protest with the help of ICTs. The emergence of cyberprotest requires the insight of the actors that something is perceived as problematic. Therefore, cyberprotest on SNS adds to the formation of critical consciousness and is likely to make students ask questions about how companies use their data on SNS.

The online behaviour of the studiVZ users in reaction to the planned change of the terms of use mainly operated on the cognitive (spreading the information) and communicative (discussing both 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 as only some thousand users joined the groups, which is no critical mass given the fact that studiVZ has several million users. Therefore, it is unclear 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 for discussion and one impressive amount of users that can engage in co-ordinated actions. A disadvantage of one overall group however is that in case that there is protest, a provider can easier shut down this group or keep it under surveillance, which allows to 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 latter's introduction. But studiVZ changed the terms so that the planned selling of user data to third parties was not included anymore and is now explicitly barred in the new terms. 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 the platform 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 (Fuchs 2010).

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

Conclusion (including future research)

The survey of SNS usage by students in Salzburg mainly focused on studiVZ because it is the most popular platform in the German-speaking world. In our study, the degree of general critical awareness of surveillance (surveillance critique index) is significantly positively correlated with the knowledge about studiVZ and the critical information behaviour on the platform. 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 study indicates that students are critical of surveillance in general, although they do not have much concrete knowledge about actual surveillance policies. Nonetheless, this critical basic attitude seems to be activated if public information and discussions make them aware that there are surveillance threats that affect them immediately, as for example on social networking sites. Therefore, one can conclude that a critical basic attitude about surveillance is not automatically transformed into critical information behaviour on SNS, but needs to be activated by public discussion. This also shows the importance of critical public discourse about surveillance and SNS.

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, and critical political parties closely observe the relationship of surveillance and SNS, and document instances where SNS 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. Examples are CorpWatch Reporting (http://www.corpwatch.org), Transnationale Ethical Rating (http://www.transnationale.org), the Corporate Watch Project (http://www.corporatewatch.org), or the Multinational Monitor (http://www.multinationalmonitor.org).

There are no easy solutions to the problem of civil rights threats 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, web platforms will continue to collect and assess certain data on them because there is an economic interest in selling user data to advertising clients and political pressure and legislation to give personal data to the police. Trying to advance critical awareness and surveiling 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, public discourse should situate the topic of electronic surveillance in the context of larger societal problems (such as the "war against terror" and corporate interests). Another option for reducing the surveillance threat of SNS 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 shows. It is advertising-free, has free access, and is financed by donations. But the difficulty is that social networking platforms have to store a 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.

There are remaining 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. Comparative studies between different localities, nations, cultures, and continents would also be interesting. The study at hand focused on students. Students are certainly early adopters of new technologies and therefore of primary interest for social research as 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 than students when it comes to the usage of technology and therefore are confronted with additional problems. Hence, 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.

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In P. Golle & G. Danezis (Eds.), *Proceedings of 6th Workshop on Privacy Enhancing Technologies* (pp. 36–58). Cambridge, UK: Robinson College.

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday 13*(3). URL: http://firstmonday.org/article/view/2142/1949.

Baker, J. R., & Moore, S. M. (2008). Distress, coping, and blogging: Comparing new Myspace users by their intention to blog. *CyberPsychology & Behavior, 11*(1), 81–85.

Ball, K. S., & Webster, F. (Eds.). (2003). *The intensification of surveillance. Crime, terrorism and warfare in the information age*. London: Pluto Press.

Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). URL: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312.

Baym, N. (2007). The new shape of online community: The example of Swedish independent music fandom. *First Monday*, *12*(8). URL: http://131.193.153.231/www/issues/issue12_8/baym/.

Beer, D. (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). URL: http://www.socresonline.org.uk/11/3/beer.html.

Beer, D. (2008a). Making friends with Jarvis Cocker: Music culture in the context of Web 2.0. *Cultural Sociology, 2*(2), 222–241.

Beer, D. (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, T. A. (2007). Harnessing collective knowledge to create global public goods for education and health. *Journal of Veterinary Medical Education, 34*(3), 330–334.

Bild-Zeitung. (2008). *Facebook, StudiVZ, Xing und Co.: Studie warnt: Daten sind nicht sicher genug*, September 29. URL: http://www.bild.de/BILD/digital/technikwelt/2008/09/26/facebook-studivz-xing-und-co/studie-warnt-daten-undfotos-sind-nicht-sicher.html.

Boyd, D. (2006). Friends, Friendsters, and MySpace top 8: Writing community into being on social network sites. *First Monday*, *11*(12). URL: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1418/1336.

Boyd, D. (2008). Why youth (heart) social network sites: The role of networked publics in teenage social life. In D. Buckenham (Ed.), *Youth, identity, and digital media* (pp. 119–142). Cambridge, MA: MIT Press.

Byrne, D. N. (2007). Public discourse, community concerns, and civic engagement: Exploring black social networking traditions on BlackPlanet.com. *Journal of Computer-Mediated Communication*, *13*(1). URL: http://jcmc.indiana.edu/vol13/issue1/byrne.html.

Cain, J. (2008). Online social networking issues within academia and pharmacy education. *American Journal of Pharmaceutical Education*, *72*(1). URL: http://ukpmc.ac.uk/articlerender.cgi?artid=1272624.

Carroll, K. S. (2008). Puerto Rican language use on MySpace.com. *Centro Journal, 20*(1), 96–111.

Charnigo, L., & Barnett-Ellis, P. (2007). Checking out Facebook.com: The impact of a digital trend on academic libraries. *Information Technology and Libraries, 28*(1), 23–34.

Cohen, N. S., & Shade, L. R. (2008). Gendering Facebook: Privacy and commodification. *Feminist Media Studies, 8*(2), 210–214.

Die Zeit (2007) *Internet Ärger um die Nutzerdaten: Das erfolgreiche Studentennetzwerk StudiVZ will endlich Geld verdienen - und handelt sich prompt Kritik von Datenschützern ein*, December 27. URL: http://www.zeit.de/online/2007/52/studivz?page=all.

Dwyer, C. (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. URL: http://csis.pace.edu/~dwyer/research/DwyerAMCIS2007.pdf.

Dwyer, C., Hiltz, S. R., & Passerini, K. (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.

Ferdig, R. E., Dawson, K., Black, E. W., Black, N. M. P., & Thompson, L. A. (2008). Medical students' and residents' use of online social networking tools: Implications for teaching professionalism in medical education. *First Monday*, *13*(9). URL: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/rt/printerFriendly/2161/2026.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*(1), 153–160.

Foucault, M. (1979). *Discipline and punish*. New York: Vintage.

Fuchs, C. (2008). *Internet and society: Social theory in the information age*. New York: Routledge.

Fuchs, C. (2010). Labour in informational capitalism. *The Information Society, 26*, (3), in press.

Gandy, O. H. (1993). *The panoptic sort. A political economy of personal information*. Boulder: Westview Press.

Goodings, L., Locke, A., & Brown, S. D. (2007). Social networking technology: Place and identity in mediated communities. *Journal of Community & Applied Social Psychology, 17*(6), 463–476.

Gormley, K. (1992). One hundred years of privacy. *Wisconsin Law Review, 1992*, 1335–1441.

Gueorguieva, V. (2008). Voters, MySpace, and YouTube. *Social Science Computer Review, 26*(3), 288–300.

Gumpert, G., & Drucker, S. J. (2000). The demise of privacy in a private world. In R. M. Baird, R. Ramsower, & S. E. Rosenbaum (Eds.), *Cyberethics* (pp. 171–187). Amherst, NY: Prometheus.

Haddon, L., & Kim, S. D. (2007). Mobile phones and web-based social networking—Emerging practices in Korea with Cyworld. *Journal of the Communications Network, 6*(2007), 5–12.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology, 51*(4), 605–622.

Harris, A., & Andrew/Lessick, S. (2007). Libraries get personal: Facebook applications, Google gadgets, and MySpace profiles. *Library Hi Tech News, 24*(8), 30–32.

Herring, S. C., Paolillo, J. C., Ramos-Vielba, I., Kouper, I., Wright, E., Stoerger, S., Scheidt, L. A. & Clark, B. (2007). Language networks on LiveJournal. In *Proceedings of the 40th Hawaii International Conference on System Sciences*. Los Alamitos, CA: IEEE Press

Hinduja, S., & Patchin, J. W. (2008). Personal information of adolescents on the Internet: A quantitative content analysis of MySpace. *Journal of Adolescence, 31*(1), 125–146.

Hodge, M. J. (2006). The Fourth Amendment and privacy issues on the "new" internet: Facebook.com and MySpace.com. *Southern Illinois University Law Journal, 31*, 95–122.

Hoofnagle, C. J., & King, J. (2008). *What Californians understand about privacy online. Research Report*. Samuelson Law Technology & Public Policy Clinic UC Berkeley Law: Berkeley, CA.

Horkheimer, M., & Adorno, T. W. (1944/2002). *Dialectic of enlightenment*. New York: Seabury.

Jones, S., Millermaier, S., Goya-Martinez, M. & Schuler J. (2008). Whose space is MySpace? A content analysis of MySpace profiles. *First Monday*, *13*(9). URL: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2202/2024.

Kim, K. -H., & Yun, H. (2007). Crying for me, crying for us: Relational dialectics in a Korean social network site. *Journal of Computer Mediated Communication*, *13*(1). URL: http://jcmc.indiana.edu/vol13/issue1/kim.yun.html.

Lange, P. (2007). Publicly private and privately public: social networking on YouTube. *Journal of Computer Mediated Communication, 13*(1). URL: http://jcmc.indiana.edu/vol13/issue1/lange.html.

Lewis, K., Kaufman, J., & Christakis, N. (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, H. (2007). Social network profiles as taste performances. *Journal of Computer Mediated Communication*, *13*(1). URL: http://jcmc.indiana.edu/vol13/issue1/liu.html.

Livingstone, S. (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, D. (2001). *Surveillance society. Monitoring everyday life*. Buckingham: Open University Press.

Lyon, David. (2003). *Surveillance after September 11*. Cambridge: Polity Press.

Lyon, D. (2005). *Surveillance society. Monitoring everyday life*. Buckingham: Open University Press.

Magnuson, M. J., & Dundes, L. (2008). Gender differences in "social portraits" reflected in MySpace profiles. *Cyberpsychology & Behavior, 11*(2), 239–241.

Marcuse, H. (1964). *One-dimensional man*. New York: Routledge.

Mazer, J., Murphy, R., & Richard, C. S. (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, M., & Ayers, M. D. (Eds.). (2003). *Cyberactivism*. New York: Routledge.
McGee, J. B., & Begg, M. (2008). What medical educators need to know about "Web 2.0". *Medical Teacher, 30*(2), 164–169.
McRobb, S., & Stahl, B. C. (2007). Privacy as a shared feature of the e-phenomenon. *International Journal of Technology and Management, 6*(2/3/4), 232–249.
Meadows-Klue, D. (2008). Falling in Love 2.0: Relationship marketing for the Facebook generation. *Direct Data and Digital Marketing Practice, 9*(3), 245–250.
Mitchell, E., & Watstein, S. B. (2007). The places where students and scholars work, collaborate, share and plan: Endless possibilities for us!. *Reference Services Review, 35*(4), 521–524.
Moor, J. H. (2000). Toward a theory of privacy in the information age. In M. B. Robert, R. Reagan, & E. R. Stuart (Eds.), *Cyberethics* (pp. 200–212). Amherst, NY: Prometheus.
Moreno, M. A., Fost, N. C., & Christakis, D. A. (2008). Research ethics in the MySpace era. *Pediatrics, 121*(1), 157–161.
Nock, S. (1993). *The costs of privacy: Surveillance and reputation in America*. New York: de Gruyter.
O'Neil, Dara. (2001). Analysis of Internet users' level of online privacy concerns. *Social Science Computer Review, 19*(1), 17–31.
OECD. (2007). Participative Web and user-created content Web 2.0, wikis and social networking. *SourceOECD, 15*(2007), i–128.
Ogura, T. (2006). Electronic government and surveillance-oriented society. In D. Lyon (Ed.), *Theorizing surveillance* (pp. 270–295). Portland, OR: Willan.
Phillips, D. J. (2009). Locational surveillance. In A. Chadwick & P. N. Howard (Eds.), *Routledge handbook of Internet politics* (pp. 337–348). New York: Routledge.
Sewell, G., & Barker, J. (2007). Neither good, nor bad, but dangerous: surveillance as an ethical paradox. In Sean. P. Hier & J. Greenberg (Eds.), *The surveillance studies reader* (pp. 354–367). Maidenhead: Open University Press.
Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *The Information Society, 19*(1), 21–32.
Stutzman, F. (2006). An evaluation of identity-sharing behavior in social network communities. *iDMAa Journal*, *3*(1). URL: http://www.units.muohio.edu/codeconference/papers/papers/stutzman_track5.pdf.
Tavani, H. T. (2008). Informational privacy: concepts, theories, and controversies. In K. E. Himma & Herman. T. Tavani (Eds.), *The handbook of information and computer ethics* (pp. 131–164). Hoboken, NJ: Wiley.
Thompson, L. A., Dawson, K., Ferdig, R., Black, E., Boyer, J., Coutts, J., et al. (2008). The intersection of online social networking with medical professionalism. *Journal of General Internal Medicine, 23*(7), 954–957.
Tom Tong, S., Van Der Heide, B., Langwell, L., & Walther, Joseph. B. (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), 531–549.
Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science Technology and Society, 28*(1), 20–36.
Turow, J., Feldman, L. & Meltzer, K. (2005). Open to exploitation: American shoppers online and offline. Research report. Annenberg Public Policy Center, University of Pennsylvania
Van de Donk, W., Loader, B., Nixon, P., & Rucht, D. (Eds.). (2004). *Cyberprotest*. New York: Routledge.
Walther, J. B., Van Der Heide, B., Kim, S.-Y., Westerman, D., & Tong, S. T. (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.
Wang, H., Lee, M. K. O., & Wang, C. (1998). Consumer privacy concerns about Internet marketing. *Communications of the ACM, 41*(3), 63–70.
Webb, M. (2007). *Illusions of security: Global surveillance and democracy in the post-9/11 world*. San Francisco: City Lights.
Zywica, J., & Danowski, J. (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.