The Internet & Surveillance - Research Paper Series

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

ISSN 2219-603X

Title: Analysis of Existing Empirical Research Methods for Studying (Online) Privacy and Surveillance

Author: Sebastian Sevignani, Verena Kreilinger, Thomas Allmer, and Christian Fuchs

Research Paper Number #10

Date of Publication: e.g. March 04, 2011

Author Institution: Unified Theory of Information Research Group

Author e-Mail: sebastian.sevignani@uti.at; verena.kreilinger@uti.at; thomas.allmer@uti.at; christian.fuchs@uti.at

Author URL: www.sns3.uti.at

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

FWF Der Wissenschaftsfonds.

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

Analysis of Existing Empirical Research Methods for Studying (Online) Privacy and Surveillance

Sebastian Sevignani, Verena Kreilinger, Thomas Allmer, and Christian Fuchs

1. Introduction

The authors of this report are research associates in the project "Social Networking Sites in the Surveillance Society". The overall aim of this research project is to study electronic surveillance on social networking sites that are used by Austrian students. For each of the following three research tasks we will identify hypotheses that will be tested in the project:

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

- Hypothesis 1: A typical attitude expressed by SNS is that they are not very concerned about becoming potential victims of individual crimes and state surveillance.
- Hypothesis 2a: SNS users typically express not much concern about the use their data for economic ends and for state surveillance.
- Hypothesis 2b: A typical attitude expressed by SNS users is that they agree that targeted advertising should be used as financing for SNS if no public funding for the operation of SNS is available. Typically they also express a preference for public funding of SNS to the advertising-financing of SNS.
- Hypothesis 2c: A typical argument of SNS student users is that they have fun in and are in favour of engaging in the lateral surveillance of other students. However, they have concerns about top-down surveillance across academic hierarchy levels (for example when students' activities on SNS are watched by professor). One typically finds support for bottom-up surveillance across academic hierarchy levels (for example when students watch the activities of professors on SNS).
- Hypothesis 3: SNS users typically express a view of privacy that is based on the control theory and privacy as extrinsic value.

Which major advantages and disadvantages of social networking platforms do Austrian students see? What is the role of surveillance in this context? What are the disadvantages, advantages that are seen by users in relation by decreased privacy? Concerning the disadvantages do they see more individual disadvantages or disadvantages for society? Is privacy considered as rather an intrinsic or rather as extrinsic value? Are disadvantages in relation to privacy described as rather intrinsic or extrin-

sic? Are privacy reduction and surveillance seen as legitimate if in return there is free access to platforms and to certain Internet services?

- Hypothesis 4: Maintaining existing relationships over spatio-temporal distances and creating new social relationships is considered as the main advantage of SNS.
- Hypothesis 5: The surveillance threat is considered as the major disadvantage of SNS.
- Hypothesis 6: Privacy is considered rather as extrinsic than as intrinsic value and as based on the control theory.

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

- Hypothesis 7: More knowledge about surveillance is significantly positively correlated to more careful information behaviour on SNS (intensity of reading the terms of use, degree of deactivation of advertising options, degree of activation of privacy mechanisms).
- Hypothesis 8: A more critical attitude towards surveillance is significantly positively correlated to more careful information behaviour on SNS (intensity of reading the terms of use, degree of deactivation of advertising options, degree of activation of privacy mechanisms).
- Hypothesis 9: There are significant differences in information behaviour on SNS between students in the hard and the soft sciences.
- Hypothesis 10: A higher degree of privacy concerns is significantly positive correlated to a more careful information behaviour on SNS (intensity of reading the terms of use, degree of deactivation of advertising options, degree of activation of privacy mechanisms).

Empirical social research and theoretical analysis will be used for finding answers to the research tasks of this project. In order to examine, which empirical research methodology might be helpful, an analysis of existing empirical research methods for studying (online) privacy and surveillance is essential. Therefore, this research report contains a documentation (section two) and a discussion (section three) of existing empirical research on privacy and surveillance.

Many authors argue that the Internet has been transformed from a system that is mainly oriented towards informational elements into a system that is more oriented on enabling communication and co-operation (Alby 2007; Beer and Burrows 2007; boyd and Ellison 2007; Burg 2003; 2004, Fuchs 2010a; Kolbitsch and Maurer 2006; O'Reilly 2005; Saveri, Rheingold and Vian 2005; Shirky 2008). Social networking sites such as MySpace and Facebook are Internet-based communication platforms that allow people to make new friends, share information, videos, music, or images, discuss with others, and stay in touch with friends, relatives, and other contacts. The notions of "web 2.0", "social software", "social media", and "social network(ing) sites" (SNS) have emerged in this context. Most approaches see the active involvement of

users in the production of content as the main characteristic of web 2.0. Regardless whether someone agrees that these transformations of the Internet have taken place, it is clear that web 2.0 activities such as creating profiles and sharing ideas on Facebook, announcing personal messages on Twitter, uploading or watching videos on YouTube, and writing personal entries on Blogger, enable the vast collection, analysis, and sale of personal data by commercial web platforms.

Thus we find it appropriate to distinguish between studying privacy and surveillance on web 1.0 and web 2.0. In section two, an overview of existing empirical research on offline, web 1.0, and web 2.0 privacy and surveillance will be given. The discussion provides theoretical considerations, a critical inquiry, and some methodological implications of empirical research on privacy and surveillance (section three).

2. Documentation of Existing Empirical Research on Privacy and Surveillance

In this section, existing empirical research on (offline, web 1.0, and web 2.0) privacy and surveillance is analysed. The following three sub-sections are structured according to this distinction. The task of this section is to give a representative, but still eclectic overview about different studies of privacy and surveillance.

2.1. Empirical Research on Offline Privacy and Surveillance

In this sub-section, existing empirical research on offline privacy and surveillance is studied.

Frequently cited consumer privacy surveys (Gandy 2003, 292) were conducted by Alan F. Westin in collaboration with the Harris-Equifax Corporation (Harris and Westin 1990; 1991). Further commercial surveys (Harris and Westin 1994; 1995; 1996; Harris Interactive 2001a; 2001b), conducted by Harris-Equifax (respectively Harris) Interactive are based on Westin's academic guidance. The Harris/Equifax surveys evaluated the public's general privacy concerns and specific privacy-related topics. Each of these surveys was conducted via telephone and each of them is statistically representative of the United States adult population.

A reason why Westin's surveys are frequent cited is that he created different privacy indexes (see in this context Gandy 2003): "Many privacy researchers around the globe are interested in using these privacy indexes as benchmarks to which they can compare their own survey results and also use these indexes to classify people in other countries" (Kumaraguru and Cranor 2005, 4). Westin, based on his survey findings, classifies survey respondents into three distinctive privacy concerned groups – namely 1) high and fundamentalist, 2) medium and pragmatist, and 3) low and unconcerned people. This classification was reflected in the development of the "General

Privacy Concern Index" (Harris and Westin 1990). People were asked binary yes/no questions:

- *if they are very concerned about their personal privacy today, if they agree strongly either that*
- *business organizations seek excessively personal information about customers or that*
- *government is still invading personal privacy of citizens since the last big privacy issue in politics (for example Watergate), and if they*
- *agree that consumers have lost all control over their information.*

Westins sees privacy threats posed by commercial organizations and state organizations. However, it can be argued that he focuses on commercial organizations because two of four questions are related to business. The answers to these questions are used in the Westin studies to assign each person to one of the three privacy concern groups: If three or all questions are answered positively, then the respondent is classified as a highly concerned and fundamentalist person. Two positive answers are indicative of a moderately concerned and pragmatic type; one question positively answered is indicative of a low grade of privacy consciousness characteristic for the group of unconcerned people.

In another one of Westin's surveys (Harris Interactive 2001a) the "General Privacy Concern Index" of 1990 was used in a different form. The "Core Privacy Orientation Index" is based on answers to the following three questions (4 point scale: "strongly disagree", "somewhat disagree", "somewhat agree", and "strongly agree"):

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

Westin uses the following definition to classify the respondents into the mentioned three groups: Privacy Fundamentalists were respondents who agreed (strongly or somewhat) with the first statement and disagreed (strongly or somewhat) with the other two statements. Privacy Unconcerned were those respondents who disagreed with the first statement and the other two statements. Privacy Pragmatists were all the other respondents.

In his 1991 survey, Westin (Harris and Westin 1991) focused on economic issues and developed the "Consumer Privacy Concern Index" by using two survey questions

with answer options on a 5-point scale. People were asked to what degree they agree (very strongly, somewhat strongly, disagree somewhat strongly, disagree very strongly disagree, neither or not sure) that:

- *'Consumers have lost all control over how personal information about them is circulated and used by companies'.*
- *'My privacy rights as a consumer in credit reporting are adequately protected today by law and business practices'.*

If a person adopts not the privacy-oriented position (agreement to the first question, disagreement to the second question), he or she was considered as having low consumer privacy concerns. If a person adopted the strongest privacy oriented position on both of the statements, the person was considered as being highly concerned. Combinations of all remaining answer options were assessed as being indicative of moderate concerns about consumer privacy. These indexes are used to predict attitudes and concerns regarding more specific privacy related issues. Such issues are "trust in organizations asking for personal information, level of comfort with organizational procedures and secondary use of data, acceptability of privacy laws and the balance of privacy with competing interests" (Smith 2006, 10). The other way round, more specific questions of privacy related issues should be contained in the general index questions.

A further important contribution of Harris and Westin to privacy research is the study of privacy concerns over time. However, Harris and Westin did not always use the same items to measure privacy concerns and did not use the same criteria of attribution in order to develop the privacy concern classification. For example, Harris and Westin tried hard not to expand the "fundamentalist" as well as the "unconcerned" group too much. These facts affect the comparability of data. The following documentation is based on data by Kumaraguru and Cranor (2005) and Harris/Westin. According to Harris and Westin, general privacy concerns measured as attitudes towards governmental and consumer privacy issues has changed over time in the following way: In 1991, about 25% of people indicated that they were very concerned about governmental and consumer privacy issues; 25% were somewhat concerned and had a "pragmatic" attitude towards these issues, 18% indicated they were unconcerned. In 1994, 51% of the respondents were very concerned, 33% were moderately concerned, and 16% indicated that they were unconcerned. In 1995, there were similar results: 47% were very concerned, 35% somewhat concerned, 18% not concerned. Consumer privacy concerns have also changed over time: In 1990, 46% of consumers were highly concerned about privacy issues, 36% were moderately concerned, and 17% were unconcerned. In 1991, 41% were highly concerned, 39% moderately or medium concerned, and 20% unconcerned. Between 1995 and 1999, several surveys showed that 25% of consumers indicated that they were highly concerned, 55% were moderately concerned and held pragmatic privacy attitudes, and 20% were unconcerned. In 2000 and 2003, the group of medium concerned individuals increased (2000: 25% highly concerned, 63% medium concerned,

12% unconcerned; 2003: 26% highly concerned, 64% medium concerned, 10% unconcerned). However in the meantime, the group of unconcerned individuals declined, whereas the group of high concerned individuals increased: in 2001, 34% were highly concerned, 58% were medium concerned, 8% were unconcerned.

An additional contribution to privacy research is that, based on an expansion of Westin's privacy typology as intimacy, solitude, anonymity and reserve (1967, 7), Harris asked US American in 1994, 2001, and 2003 for assessing privacy concerns. People were asked to express their commitment to the following statements that describe various types of privacy; statements were scaled by a 5-point Likert scale from "strongly agree" to "strongly disagree" (see Zureik 2004b, 4):

- *Not being disturbed at home (territorial privacy)*
- *Not being monitored at work (bodily privacy)*
- *Being in control of who can get information about you (informational privacy)*
- *Having someone watch you or listen to you without your permission (privacy of communication)*
- *Controlling what information is collected about you (informational privacy)*
- *Being able to share confidential matters with someone you trust (privacy of communication)*
- *Being able to go around in public without always being identified (territorial privacy)*
- *Having individuals in social and work settings not ask you things that are highly personal (privacy of communication)*
- *Being able to have times when you are completely alone, away from anyone else (territorial privacy).*

In 2000-2001, a survey was conducted by Harris and the Private Leadership Initiative (PLI), a partnership of CEOs from 15 major corporations and 9 leading business associates. Its purpose was "to track changes and trends in attitudes, behaviors, experiences, and expectations of consumers with regard to online and offline privacy." (Harris Interactive 2001b) The survey was representative of the general and the online population in the Unites States and took place in three waves. In the first wave 1026 adults (aged 18 and older) were interviewed by telephone and 2087 adults were asked to fill out a questionnaire online. In the second wave of this survey a national cross section of 1001 adults were interviewed by telephone and 2180 adults were interviewed online. This part of research focuses on the complicated interrelationship between business, government, and the individual consumer; it "explores consumer confidence in sharing personal information online and offline, concerns related to the collection and use of personal data and the perceived benefits of personalization" (Harris Interactive 2001b). The whole survey found in respect of privacy in general (offline or offline and online) that the trust in either business or government for protecting privacy is low. Respondents indicated that individuals bear the most responsibility for protecting privacy. However, individual consumers feel

not to have enough control to do so. People feel their privacy is better protected when using offline media than online media. Online users are more willing to provide more information when asked for by online as well as off-line companies, than individuals who do not use the Internet. Only about half of the (online and offline) respondents see personalization as a good issue. Within this half, the majority does not value benefits of economic and advertising aspects of personalization, such as advanced information about new products, more product information, easier buying processes, faster transactions, discounts, and improved customer service. Adults protect their privacy by taking proactive steps such as refusing to give too much personal information, asking companies to remove their personal information from marketing lists, and asking a company not to sell or give their names to other companies.

Also a third wave of the survey was conducted that focused exclusively on privacy notices and "explores consumer experiences with privacy notices and attitudes towards format and content" (Harris Interactive 2001b). 2053 adults were asked to fill out a questionnaire online. This part of the survey found that the overwhelming majority of consumers were not confident with existing privacy notices, off-line and online. The majority of respondents preferred to read shorter notices (80% of the respondents indicated this) and wanted to see some comparability or consistency of privacy notices (70% said this). Concerning the content of privacy notices, respondents are mostly interested in information about how to remove their personal information from the companies' databases and how personal information is sold and shared with other companies.

In 2006, an international survey on privacy and surveillance was conducted by several scholars of "The Globalization of Personal Data" (GPD) project at Queen's University, Canada. Participating countries were Brazil, Canada, China, France, Hungary, Mexico, Spain, and the Unites States. The "focus in this study extends beyond informational privacy to include territorial, communicational, and body or physical privacy" (Zureik 2004a, 7). The GPD survey is divided in two parts: The first one includes qualitative research, namely focus group interviews in each of the eight participating countries in order to develop a precise questionnaire for the second, quantitative part of the study (Zureik et al. 2010, ix-x).

Qualitative research was conducted via focus groups interviews. Interviews with each focus group (approximately 15 participants, based on four actor categories, namely workers, consumers, citizens, and travellers) were conducted by commercial research institutes, which "are well known for the public opinion polling they do on privacy related issues" (Zureik, Harling Stalker, and Smith 2006, 13). The focus groups were balanced regarding various demographic characteristics, but not representative. The interviews were videotaped, transcribed into English, and summarized. Focus group interviews were conducted for two reasons: First, they helped "to identify key concerns about privacy present in the various countries" (Zureik, Harling

Stalker, and Smith 2006, 13). Therefore, participants were asked for ranking their perception of the importance and the threat of different types of privacy (bodily, communication, information, territorial). One result was that the study should focus on informational privacy. Second, focus group interviews helped to hypothesize the results of the survey and clarified how the results might vary among different cultures and countries.

We now document qualitative questions, which were used within the different parts of the focus groups interviews:

- *"Introduction (5 minutes): Moderator explains the purpose of the research and who is the client; Mention that the discussion is being audiotaped as the moderator cannot take good notes during the focus group; Mention that participants are being observed by members of the research team; Confidentiality: Explain that the findings from the focus groups are kept confidential. No full names will be associated with any information provided in this discussion group. The report will simply describe patterns of opinions over the series of focus groups; Explanation of format and 'ground rules': there are no wrong answers/no right answers, okay to disagree, individuals are asked to speak one at a time; Moderator's role: raise issues for discussion, watch for time and make sure that everyone gets a chance to speak; Ask participants if they have any questions before beginning; Participant introductions: ask participants to introduce themselves by their first name only and to say a little bit about their background (e.g., occupation/status)." (Ekos 2004, 17)*

- *"Perceptions and Experiences with Privacy Issues (35 minutes): When you hear the word 'privacy', what is the first thing that comes to mind? [Moderator instructs participants to write down the first thing that comes to mind.]; And when you hear the word 'security', what is the first thing that comes to mind? [Moderator instructs participants to write down the first thing that comes to mind.]; Respondents are then asked to read what they wrote down about 'privacy' and 'security'; People often talk about privacy as a value. What is a value [PROMPT: freedom, equality are often cited as values]? What about privacy as a value?; In our surveys, we often ask people about privacy, and whether or not they feel that they have less privacy in their daily life than they did five years ago. How would you answer this question? A) Can you tell us why you feel that way? B) In what areas do you have less privacy? C) How concerned are you about your privacy today? What kinds of things do you do to protect your privacy? Where do you generally get your information about privacy issues? Have you ever discussed these issues with family, friends? How have your views changed in the past five years? In what ways? What prompted these changes? Is anything different since September 11th? Has anything you have seen in the media (TV, radio programming, newspaper, magazines, online information or advertising) prompted these changes? How so? D) Have you ever experienced a serious invasion of privacy? What kind of invasion of privacy was it? Can you give me some examples*

of privacy invasions? Invasions in your day-to-day lives? Invasions by government? Invasions by companies? Invasions in the workplace? What are some other ways that your privacy could be compromised? [Prompt if necessary: identity theft, credit information, credit card, financial information, surveillance cameras, tracking of purchases]. E) Are some groups in society more susceptible to invasions of privacy than others? Which groups? [PROMPT: Low-income, visible minorities, ethnic groups] Why do you say that?" (Ekos 2004, 18-19)

- *"Expectations Regarding Privacy Issues in the Future (15 minutes): How likely is it that you will actually experience a serious invasion of your personal privacy over the next five years? What type of invasion could you see happening? Compared to today, do you think that the threat of an invasion of your personal privacy will be greater or less in ten years from now? Why do you say that? What do you think may not be as private in the future? If I asked you to pick one thing, what would you say is the biggest threat to your privacy in the future? How do you think technology will affect your personal privacy in the future?" (Ekos 2004, 19)*

- *"Awareness of and Attitudes towards Privacy Technologies and Legislation (30 minutes): A) Technologies: How much do you rely on electronic or computer-based technology in your daily life, either at home or at work? What types of technology do you use? How confident would you say you have enough information to know how technology might affect your personal privacy? What about the Internet? How could the Internet affect your privacy? And what about email? Are you aware of things that you could do to protect your privacy while on the Internet? Have you ever done anything to protect your privacy while on the Internet? Have there been any changes with respect to the use of these technologies by companies/governments in the past few years when it comes to your privacy? In what way have things changed? What do you think prompted this change? B) Legislation: What things exist to protect your privacy today? What laws exist? Are you aware that there are federal privacy laws that place strict restrictions on how federal government departments use personal information, including restrictions on the sharing of personal information? To what extent do you believe these laws are effective at protecting your privacy? What about laws that place restrictions on how companies use personal information, including restrictions on the sharing of personal information? To what extent do you believe these laws are effective at protecting your privacy? [As some of you mentioned] some measures aimed at increasing security are, at times at the expense of privacy. Do you think this is currently the case? Specifically, what security measures compromise privacy? On balance, do you feel these measures aimed at increasing security are justified? What about in the future? Do you expect the emphasis will be more on 'security' or 'personal privacy'?" (Ekos 2004, 20-21)*

- *"Privacy Issues Specific to Workers (25 minutes): To what extent do you think companies keep track of the activities of employees while they are in the workplace? Are*

they tracking how much time employees spend online, maintaining a list of websites employees visit and information entered? Emails sent or received? Should they be allowed to monitor these types of activities of their employees? What types of activities? Why? Why not? What is and isn't personal information in the workplace? Do you know if your employer uses any methods to track the actions of their employees? How do you feel about this? Do you believe businesses are required to inform employees and prospective employees of different methods they may use to monitor workplace activities? Should employers be able to monitor all their employees equally or should they be able to target or exempt individuals or groups of employees from monitoring?" (Ekos 2004, 21)

- *"Privacy Issues Specific to Consumers (25 minutes): How many of you have ever participated in a customer loyalty program such as Airmiles? What is the purpose of these programs? Why do you participate? What type of personal information do they collect? What do they do with this personal information? Can they sell this personal information to other companies? Under what circumstances can they? [FOR THOSE IN LOYALTY PROGRAMS] Have you given consent? As some of you may know, when individuals take part in a loyalty program such as Airmiles, each time they use their card to collect points, the Airmiles company keeps track of the items they have purchased. These companies can then sell this 'purchasing behaviour' information to other companies participating in the Airmiles loyalty program. What do you think of a company being able to track purchases? What do you think of them being able to transmit that information to other companies? What kinds of things is it ok for companies to monitor?" (Ekos 2004, 22-23)*

The qualitative research resulted in several implications for quantitative research; we provide examples of these results in detail because in the literature only a few qualitative survey results can be found (Ekos 2004, 15):

- "Privacy is not something that most individuals will think about on a day-to-day basis, suggesting the need to design a number of introductory questions to set the context. This is likely to be even more important in countries where privacy rights and laws are not as well as established compared to the westernized countries (…).
- The findings reinforce the complexity and context driven nature of privacy concerns and the fact that privacy (and security) will mean different things to different individuals within the same country, let alone across countries. This reinforces the value in having 'vignettes' to describe some examples to gauge attitudes on a comparable basis across countries.
- It is also clear that there is a continuum on the privacy protection front, where the perceived roles of the state and the individuals will differ. For example, respondents may have perceptions about the role of the state when asked broadly, but

would make notable distinctions in relation to health information and purchasing habits, for example.
- In addition to the basic demographics, there may be value in considering the addition of various 'background' types of questions important from an analytical point of view. Some examples include having experienced invasions of privacy, confidence in governments to follow laws, sense of individual responsibilities in protecting their own privacy, and proxies for specific actions that individuals have taken to protect their privacy (e.g., withholding information)."

On the content level, the qualitative research resulted in the following findings (Ekos 2004, 14):
- "Personal privacy is seen as eroding, driven mainly by technological evolution.
- Most participants appear resigned to a future with less privacy.
- Participants tend to pragmatically assess the acceptability of privacy invasions or intrusions based on key criteria (e.g., purpose, effectiveness, cost, disclosure and awareness). Awareness is a particularly important issue given that it is often low.
- Few participants spoke of personal privacy as a value or in philosophical terms (e.g., linked to civil liberties, freedom or democracy). Instead, participants view personal privacy as a "right" that can only be effectively safeguarded by the individual through knowledge, awareness and, ultimately, vigilance and action/redress.
- Governments are seen as providing legislative and other protections (e.g., Privacy Commissioners, Ombudsmen), but are not perceived to be in a position to effectively monitor compliance or enforce (i.e., there are simply too many transactions/instances, and not enough resources).
- At the same time, the credibility of government as privacy guardian is diminished by view of government as a potentially prime invader of personal privacy.
- Despite primacy accorded individual action, most acknowledge that they have adopted a laissez-faire attitude to their personal privacy, relying on government and the good will of the organizations with which they do business.
- The proliferation of technology and instances where personal information or other forms of personal privacy are at stake have become too numerous and complex for the average person to be vigilant about.
- Ambivalence and stoicism is reinforced by the fact that most have yet to suffer serious personal consequences of a privacy invasion (e.g., banks absolve clients of liability for fraudulent credit card use)."

The quantitative part of the GDP survey included several topics, which are relevant for our own research, such as knowledge about surveillance technologies, knowledge of laws protecting personal information from governmental and commercial use, control of personal information, people's trust in companies and governments, proactive steps in order to protect their people's personal information, privacy on the Internet, attitudes towards information sharing, and consumer privacy. A total of 9090 re-

spondents were interviewed, either personally (Mexico and Brazil) or by using the Computer Assisted Telephone Interview (CATI) technology (U.S.A.; France, Spain, Hungary, and China). CATI "respondents were screened to ensure nationally representative samples based on gender, age and regional distribution, except for China where respondents were selected from 7 major cities" (Chan et al. 2008, 6). For personal interviews "urban samples were used instead of a nationally representative sample"(Chan et al. 2008, 6). In Japan, respondents were asked to complete an online questionnaire. The respondents were selected in order to ensure an even distribution of gender and age (Chan et al. 2008, 6). The survey questionnaire includes general questions, such as age, gender, education, employment, occupation, income, language, ethnicity, air travel, purchase over the internet, contact with government, and use of a computer and the Internet.

In the following, several items and corresponding results of the survey are documented. The full questionnaire of this international survey is publicly accessible (see Zureik et al. 2010, 361-382); it can also be found in the Appendix (Appendix A) of this report.

The degree of knowledge of various surveillance technologies (Internet, data mining, GPS, biometrics, etc.) was polled:

- *"In general, how knowledgeable are you about each of the following? Would you say you are very knowledgeable, somewhat knowledgeable, not very knowledgeable or not at all knowledgeable? First is [Read first item. Record response. repeat scale as necessary] Next is [Read next item. Record response. check one box for each row]" (Zureik et al. 2010, 363)... (answer opportunities were: "very knowledgeable", "somewhat knowledgeable", "not very knowledgeable", "not at all knowledgeable", "don't know/unsure").*

Provided items were: Internet; Global Positioning System (GPS) used in automobiles; Radio Frequency Identification (RFID) Tags on consumer products; Closed Circuit Television (CCTV) in public spaces; Biometrics for facial and other bodily recognition; Data mining of personal information.

Referring to the Internet, findings show that among all respondents 26,8% were very knowledgeable and 37,5% somewhat knowledgeable; referring to data mining only 4,7% were very knowledgeable and 16,8% somewhat knowledgeable (Chan et al. 2008, 8-9).

The researchers asked the respondents about their knowledge of laws protecting personal information from governmental and commercial use:

- *"How knowledgeable are you about the laws in [Insert name of country where interview is conducted] that deal with the protection of personal information in government departments and private companies? First, let's start with [Insert one of gov't dept or private companies. ramdomize]. Would you say you are [Read list. Record*

one response]. And how about [Insert gov'r dept or private companies - whichever wasn't asked first] [Read response list if necessary. Record one response]" (Zureik et al. 2010, 364) ... (answer opportunities were: "very knowledgeable", "somewhat knowledgeable", "not very knowledgeable", "not at all knowledgeable", "don't know/unsure").

In addition, people's perception of how effective existing laws are was examined:

- *"To what extent do you believe laws are effective at protecting your personal information that is held by government departments and private companies? First, let's start with [Insert item very/somewhat knowledgeable in Q3. Insert in same order as Q3]. Do you believe the laws are [Insert scale. record one response]. And how about [Insert next item very/somewhat knowledgeable in Q3.] Do you believe the laws are [Read scale. Record one response only]" (Zureik et al. 2010, 365)... (answer opportunities: "very effective", "somewhat effective", "not very effective", "not effective at all", "not sure").*

The results show that 4,6% of the respondents were very knowledgeable and 32,1% somewhat knowledgeable of laws dealing with personal information protection in government departments. 56% of the respondents considered the existing laws as (somewhat or very) effective. Respondents were less knowledgeable of laws regulating the private sector: 3,9% were very knowledgeable, 28,1% were somewhat knowledgeable of laws dealing with personal information protection in private companies; 52,3% of the respondents considered the existing laws for the private sector as (somewhat or very) effective.

Control theories of privacy stress the importance of the individual's control of privacy. Therefore people's perception of control over personal information was examined in the GDP survey. People were asked:

- "*To what extent do you have a say in what happens to your personal information?" (Zureik et al. 2010, 364) (answer opportunities: "complete say", "a lot of say", "some say", "no say", "not sure").*

19,2% felt they have some say, 23,7% felt they have no say, 39,4% felt they have complete say, and 15,3% felt they have a lot of say in what happens with their personal information (Chan et al. 2008, 12).

The survey shows that a minority of respondents trust "that their government or private companies will do an appropriate job of protecting their personal information" (Chan et al. 2008, 13). Participants were asked how much they trust their government to establish/maintain the right balance between individual rights and security:

- *"When it comes to the privacy of personal information, what level of trust do you have that the [Insert country of interview] government is striking the right balance between national security and individual rights? Do you have a" (Zureik et al. 2010,*

365)… (answer opportunities: "very high level of trust", "reasonably high level of trust", "fairly low level of trust", "very low level of trust", "not sure").

According to trust in the private sector, people were asked to reply to the following question:

- *"What level of trust do you have that private companies, such as banks, credit card companies and places where you shop, will protect your personal information? Do you have a [Read list. Record one response]" (Zureik et al. 2010, 365)… (same answer opportunities as above).*

People trust private companies a bit more than governments; 7,3% had a very high level of trust and 37,4% had a reasonable high level of trust in private companies.

People were asked about proactive steps that can be taken in order to protect their personal information:

- *"Have you ever done the following for the purpose of protecting your personal information? [Read list. Record yes or no for each) [Randomize list]" (Zureik et al. 2010, 366) (answer opportunities were "yes", "no", and "don't know/not sure").*

Provided items were (Zureik et al. 2010, 366):

- *"Refused to give information to a business because you thought it was not needed?"*
- *"Refused to give information to a government agency because you thought it was not needed?"*
- *"Asked a company to remove you from any lists they use for marketing purposes?"*
- *"Asked a company not to sell your name and address to another company?"*
- *"Asked a business you were thinking of dealing with about policies on the collection of consumer information?"*
- *"Asked a company to see what personal information besides billing information they had about you in their consumer records?"*
- *"Purposefully gave incorrect information about yourself to a marketer?"*
- *"Purposefully gave incorrect information about yourself to a government agency?"*
- *"Read the on-line privacy policies at websites when making a purchase from a private company?"*
- *"Read the on-line privacy policies at government websites when sending them information electronically?"*

Considering results of proactive steps against economic interests in particular, the survey found that 51,5% of the respondents refused to give information to a business (in comparison, to government: 22,4%), 33,6% have asked a company to remove their data from marketing lists, 35,6% have asked a company not to sell information to another company, 17,6% have asked a business about their policies on the collection of consumer information, 12% have asked companies to see what personal information they had in records, 15,3% have purposefully provided incorrect information to a marketer (in comparison to providing purposefully false information to government: 4,2%), and 33,2% have read on-line privacy policies on websites when mak-

ing a purchase (in comparison, on government websites: 24,2%) (Chan et al. 2008, 14-15).

Also experiences with surveillance were assessed:

- *"Have you personally to the best of your knowledge, ever experienced any of the following? For each item, please indicate yes, no or not sure. If you have never experienced a particular situation, or if a situation does not apply to you, please say "no". [Read list. Record one response for each) [randomize list]." (Zureik et al. 2010, 366-367) (answer opportunities were "yes", "no", and "don't know/not sure").*

Provided items were (Zureik et al. 2010, 367): "Detention at a border checkpoint resulting in a search", "Detention by airport officials resulting in not being able to board the airplane", "Detention by airport officials resulting in being denied entry into a country", "Victim of identity theft (e.g. someone uses your name)", "Victim of credit card fraud", "Your personal information monitored by a government agency", "Your personal information monitored by an employer", and "Your personal information sold by a commercial business".

The list of items above shows that the GPD project focused on state surveillance. 18,9% of the respondents said that their information had been sold by a commercial business (Chan et al. 2008, 16-18).

The survey also included a thematic focus on privacy on the Internet. People were asked:

- *"When it comes to privacy, how worried are you about providing personal information on websites, such as your name, address, date of birth, and gender?" (answer opportunities: "very worried", "somewhat worried", "not very worried", "not worried at all"; Chan et al. 2008, 20) and*
- *"Who do you think should have the most say over how companies use their websites to track people's activities and personal information online?" (answer opportunities: "government", "companies that run the website", "people who use the website", "not sure"; Chan et al. 2008, 20).*

Results show that 26,6% were very worried, 37,2% were somewhat worried, 18,4% were not very worried, and 15,0% were not worried at all about providing personal information on websites (Chan et al. 2008, 20). No details were asked about the kind of websites (government or business, etc). About 40% of the respondents thought that governments should determine how companies use their websites to track people's activities and personal information online. About 20% thought that business should be in control itself without state regulation and about 30% thought that people should determine how companies use their websites to track people's activities and personal information online (Chan et al. 2008, 20).

Assuming that media coverage of surveillance and privacy issues will increase respondents' awareness of these topics, it was assessed how much coverage had been seen or heard and how individuals thought about media coverage of privacy and surveillance:

- *"How much coverage have you seen or heard through the media (TV, radio, newspapers, magazines, online information, advertisements) regarding concerns about the safety of your personal information? Do they provide [Read list. Record one response]" (Zureik et al. 2010, 368)… (answer opportunities: "a lot of coverage", "some coverage", "not much coverage", "no coverage at all", "not sure").*
- *"Would you say the media pays: [Read list. Record one response] [Randomize order of first and second items]" (Zureik et al. 2010, 369)… (answer opportunities: "more attention to stories about terrorism", "More attention to stories about private sector violation of personal privacy of consumers", "Pays equal attention to both", and "not sure").*
- *„When it comes to media coverage of privacy of personal information, in your opinion, how much attention does each of the following groups receive by the media? Please use a scale from I to 4 where I represents low amounts of attention and 4 represents high amounts of attention? If you are unsure, please say "don't know". First is [Read first item. Repeat scale if necessary]. Next is [Insert second item. Repeat scale if necessary]" (Zureik et al. 2010, 369).*

According the last question, provided items were (Zureik et al. 2010, 369): "Low-income persons", "Visible minorities", "Middle class people", "Celebrities", "Government officials", "People like you", "Immigrants", "Homeless", "High-income people")

13,3% of the respondents indicated that they had been exposed to a lot of media coverage about the personal data security, 35% reported that it had been some media coverage, 35,5% said that it had been not much media coverage, and 15,2% reported that they had seen or heard no media coverage regarding personal data security (Chan et al. 2008, 21-22). 40,9% of respondents thought that the media pay more attention to stories about terrorism; only 12,3% of the respondents thought that the media pay more attention to stories about privacy invasion by companies; and 30,9% thought that the media pay equal attention to both (Chan et al. 2008, 22). When it comes to specific groups the media have given account to, the majority of citizens was in agreement that the "media focuses more on celebrities, government officials and high-income groups than on the poor and the disadvantaged" (Chan et al. 2008, 23)

Assessing attitudes towards information sharing (for example between government and businesses) was a further aim of the survey (Zureik et al. 2010, 370-371):

- *"To what extent do you think it is appropriate for a government agency to share citizen's personal information with third parties, such as other government agencies, foreign governments and the private sector?"*

- *"To what extent do you think it is appropriate for a private sector organization to share or sell its customers' personal information with third parties, such as the national government, foreign governments and other private sector organisations?"*

The following answer opportunities and items were provided (in case of governmental information sharing, "organization" was replaced by "government", "consumer" was replaced by "citizen", sharing "with the national government" was replaced by "other government agencies", and sharing "with other private sector organizations" was replaced by "the private sector") (Zureik et al. 2010, 371): "Yes, it is the organization's right under all circumstances", "Yes, if the customer is suspected of wrong-doing", "Yes, as long as the organization has the expressed consent of the customer", "No, under no circumstances should organisations share information about their customers", and "not sure". These answer opportunities are related to the following items: sharing "with national government", "with foreign governments", and with other private sector organisations".

The majority (38,1%) of respondents did not want (under no circumstances) governments to share information about citizens with the private sector. 29,4% said yes, government can do this, as long as the government has obtained consent of the citizens, 20,5% said yes, if the citizen are suspected of wrong-doing, and 4,3% said that it is the government's right under all circumstances) (Chan et al. 27). Vice versa, about 30% said that under no circumstances should private sector organizations share or sell customers' personal information with governments. 46,7% were opposed to the sharing or selling of personal information between private sector organizations: 32,8% said yes, this should be possible as long as the organization has expressed consent of the consumer; 15,4% said yes, if the consumer is suspected of wrong-doing, and 3,4% said yes, it is the organization's right under all circumstances) (Chan et al. 28).

Finally, concerns towards consumer surveillance were assessed. Respondents were asked:

- *"Many businesses create profiles about their customers that include information about purchasing habits, personal characteristics and credit history. How acceptable to you would it be for a business to use information from your customer profile to inform you of products or services that they think would be of interest to you? Do you feel it is [Read list. Record one response]" (Zureik et al. 2010, 374)… (answer opportunities: "very acceptable", "somewhat acceptable", "somewhat unacceptable", "not acceptable at all", "not sure").*

The majority responded that creating customer profiles would be acceptable: 10,3% said that it would be very acceptable, 45,9% said that it would be somewhat acceptable, 21,7% said that it would be somewhat unacceptable, and 21,5% said that it would not be acceptable at all (Chan et al. 2008, 34).

The aim of the quantitative survey conducted by Mary Culnan is to explore attitudes towards secondary information use in the context of direct mail advertising among young customers. Culnan seeks "a preliminary understanding of how overall attitudes toward information privacy and direct marketing can differentiate consumers with positive attitudes from consumers with negative attitudes toward the secondary use of personal information for direct marketing" (Culnan 1993, 343). In this study, (informational) privacy is measured as individual control over personal information. Two research questions are raised: "Do individuals with more positive attitudes toward secondary information use differ from those with more negative attitudes based on (1) their attitudes toward direct marketing and (2) their concern for privacy?" (Culnan 1993, 347). The instrument of the survey was a questionnaire. After pretesting it in a focus group with MBA students being familiar with privacy issues, the final questionnaire was administered to 126 (N) U.S. undergraduate information systems students. The survey instrument borrows in large extents from former surveys conducted by Harris/Equifax. Demographic data was collected in order to determine respondents' experience as consumers and with direct marketing (credit card use for payments, names being placed on mailing lists, etc.).

The majority of respondents had experienced secondary information use in the context of direct mail advertising. Concerns about the secondary use of personal information (first independent variable, included overall concern, control, and unauthorized use of personal information) were measured using five items. Each item had answer opportunities on a 5-point Likert-scale. The items were partly taken from former surveys by Harris/Equifax (items 1, 2, and 3) and Smith (items 4 and 5) (Culnan 1993, 350):

- *"I am concerned about threats to my personal privacy".*
- *"Consumers have lost all control over how personal information is used".*
- *"Americans begin surrendering their privacy the day they open their first charge account".*
- *"Companies should not use personal information for any purpose other than the one authorized".*
- *"A company should not share personal information about me without my permission".*

Attitudes toward direct marketing (second independent variable, includes overall attitude toward mail, benefit of mail shopping, cope with mail, and opt out) were measured in two ways. First, an item taken from a Harris/Equifax survey was used to find out on a general level if direct marketing activities are viewed as a benefit or as a privacy invasion. Participants were asked "whether, overall, they viewed the receipt of catalogs and mail offers at home as 'primarily as useful,' 'rarely use but no problem,' 'more as a nuisance,' or 'more as a privacy invasion'" (Culnan 1993, 359). The survey showed – in accordance with the results of the Harris/Equifax survey – that the overwhelming majority (72%) viewed direct marketing activities as useful or not

problematic; while only 2% viewed them as privacy invasions. Second, seven items (again partially borrowed from former Harris/Equifax surveys; measured by a 5-point ascending Likert scale) were used to find out respondents' attitudes towards control and benefits of direct marketing activities (Culnan 1993, 350):

- *"Shopping at home saves time over shopping in a store".*
- *"I enjoy being able to shop by mail or phone when It's convenient for me".*
- *"I would be annoyed if I could not receive mail offers or catalogs geared to my interests".*
- *"It's not a problem to receive catalogs that don't interest me; I just throw them away".*
- *"It annoys me that I receive so many unsolicited catalogs and mail offers that don't interest me".*
- *"If I choose, I can have my name removed from mailing lists".*
- *"When I receive mail offers I don't want, I am aware of procedures that allow me to remove my name from these mailing lists".*

In addition, respondents were asked for their awareness of consumer privacy issues by using an item from former Harris/Westin surveys. People were asked:

- *"How much they have heard or have read during the past year about the use and potential misuse of computerized information about consumers" (Culnan 1993, 352).*

A 5-point Likert scale running from "a great deal" to "nothing at all" was used.

Respondents were also asked to respond to two open-ended questions: First, an example of a real or hypothetical situation involving personal information that violates their privacy should be given by the respondents. Second, respondents should list types of personal information "one company should never share with another company unless you have given them your written permission". All results were correlated with the demographic data in order to get insights on the influence of respondents' life experience on privacy concern. A grocery's frequent shopper program (the membership application was given to the respondents) was used as focus material in order to measure attitudes towards secondary information use (dependent variable). One question about respondents' overall view of direct marketing plus 11 items asking questions about different direct marketing activities were developed (4 point Likert scale from "primarily useful" to "an invasion of privacy").

A typical question used in the survey is the following one (Culnan 1993, 353):

- *"You regularly buy Diet Coke, You receive coupons in the mall from Pepsi-Cola for Diet Pepsi, How do you view this use of personal information?"*

The full questionnaire of this part of Culnan's survey can be found in the Appendix (Appendix B).

As a result, respondents were split into two groups according to whether they see direct marketing as useful or as a privacy invasion. A discriminant analysis was used to answer the research questions: privacy measured as control, perceived benefits of shopping by mail, and ability to cope with unwanted account differences in the attitudes towards secondary information use. “The remaining variables (overall concern for privacy, privacy measured as unauthorized secondary use, overall attitude toward direct mail, ability to "opt out," and having experienced an Invasion of privacy)” (Culnan 1993, 355) were not significant. In addition, the responses to the two open-ended questions showed that transfer of information across organizations, especially financial, medical or lifestyle information were perceived as the most important privacy invasions (31%). The types of information that respondents thought should never be shared by organizations are financial information (71%), information on lifestyle or "vices" (23%), demographic information (including race or marital status; 18%), medical information (17%), and information on an individual's buying practices (8%). 12% said that no personal information at all should be shared without permission, 4% felt that any personal information could be shared without permission.

In 1999, Culnan and Armstrong conducted a survey in order to test their overall hypothesis “that consumers will be willing to disclose personal information and have that information subsequently used to create profiles for marketing use when their concerns about privacy are addressed by fair procedure“ (Culnan and Armstrong 1999, 104). Procedural fairness refers to the control theory of privacy (for example “opt out” opportunity): “Fair information practices are procedures that provide individuals with control over the disclosure and subsequent use of their personal information“ (Culnan & Armstrong 1999, 107). The survey refers fairly to former Harris/Equifax surveys and was sponsored by Privacy and American Business. Harris/Equifax collected the data via telephone and used a sample of 1000 (N) U.S. adults aged 18 years and older. Results of the study were based on secondary data analysis of a Harris/Equifax survey designed to measure public opinion. Culnan & Armstrong provided three hypotheses that they tested (1999, 108-109):

- “H 1. When people are not explicitly told that fair procedures will be employed for managing their personal information, people with a greater concern for privacy will be less willing to have their personal information used for profiling.”
- “H 2. When people are explicitly told that fair procedures will be employed for managing their personal information, privacy concerns will not distinguish people who are unwilling to be profiled from those who are willing to have their personal information used for profiling.”
- “H 3. Prior experience with targeted marketing will distinguish people who are willing to have their personal information used for profiling from those who are not willing.”

In order to test these hypotheses independent and dependent variables were identified. The dependent variable was the willingness to have one’s personal information

used to develop profiles for targeted marketing in general and in combination with fair information practices. Respondents were asked to express their willingness and the importance of single fair information practices on a 4 point Likert scale (from "not at all interested" to "very interested", respectively from "not important" to "very important"). The independent variable was the behaviour that indicates a concern for privacy (operationalized by using three dichotomous variables that measured an individual, which taking steps to restrict the disclosure of personal information) and prior experience with direct marketing (measured by dichotomous variables as well). Culnan and Armstrong argue that additional demographic data and data concerning the experience with direct marketing not necessarily needs to be collected because demographic and experience differences are already captured by the behavioural and attitudinal variables (Culnan and Armstrong 1999, 110). A discriminant analysis was applied in order to get the following results: All three hypotheses were supported, which means "privacy concerns can be addressed by explicitly telling customers that the company observes fair information practices" (H1, H2) and "people who are willing to be profiled for marketing purposes are more likely to have prior experience with direct marketing than people who are not willing" (H3) (Culnan and Armstrong 1999, 112).

Dommeyer and Gross conducted a study that "focuses on the consumer's knowledge, awareness, and use of strategies that could minimize privacy invasions by direct marketers" (2003, 35). They provide am "updated account of current consumer knowledge and behaviors" (Dommeyer and Gross 2003, 36). In order to do so, a quantitative survey was conducted. The poll was representative of U.S. citizens; however further statistical calculations based on the poll were not representative. The complete sample of the survey included 520 consumers, to whom the questionnaire was sent by mail. The respondent rate was 30% (N=137).

The survey consisted of a four-page long questionnaire containing four sections. The first section included three questions about attitudes towards different direct marketing activities, namely "'receiving catalogs in the mail', 'receiving advertisements in the mail', and 'receiving calls from telephone solicitors'"(Dommeyer and Gross 2003, 40). Answer opportunities were provided by using a 9-point Likert-scale, running from 'like' to 'dislike'.

The second section included 10 statements about the knowledge of how direct marketing practices affect consumer privacy (answer opportunities: "true", "false", "don't know") (Dommeyer and Gross 2003, 41):

- *"If you tell a telephone solicitor from a commercial organization that you do not want to receive any more calls from him or his company, he is legally required to honor your request. (True)"*
- *„If you call a company's "800" or "900" number, that company cannot identify the number you are calling from unless you reveal the number to them. (False)"*

- *„Suppose that your local video store wants to sell a customer mailing list (i.e., a list that contains its customers' names, addresses, and the types of videotapes they rent) to other marketing firms. Your video store can legally add your name to this type of mailing list without getting your oral or written permission. (True)"*
- *„If you do not fill out and return a product registration form, you will not be covered by the manufacturer's product warranty. (False)"*
- *„Telephone solicitors are able to call people who have an unlisted telephone number. (True)"*
- *„If you subscribe to your telephone company's complete "call blocking" service, your telephone number can not be identified by any company you call unless you reveal the number to them. (False)"*
- *„When you sign up for the Direct Marketing Association's Mail Preference Service, your name will be removed from some companies' mailing lists. (True)"*
- *„If you tell a caller from a nonprofit organization that you do not want to receive any more calls for charitable contributions from his organization, he is legally required to honor your request. (False)"*
- *„When you sign up for the Direct Marketing Association's Telephone Preference Service, your name will be added to some companies' calling lists. (False)"*
- *„If you write to the publisher of Time Magazine, a general interest magazine, and ask that your name be removed from their mailing list, the publisher is legally required to honor your request. (False)"*

In the third section, 26 different privacy protection strategies were presented. Respondents were asked to indicate their degree of familiarity with each strategy (answer opportunities: "unaware of strategy", "aware, but not used", "have used strategy") (Dommeyer and Gross 2003, 42):

- *"I do not fill out product registration forms."*
- *"I screen my telephone calls with an answering machine."*
- *"When calling a company to order something, I don't give out my home telephone number unless I think it's absolutely necessary."*
- *"I do not have my telephone number printed on my personal checks."*
- *"When filling out a purchase form, e.g., a catalog order form or an application for a buyers club, I will check the box at the bottom of the form that tells the company that I do not want to receive coupons, advertisements, or other offers."*
- *„I do not enter sweepstakes or contests when I would be required to provide my address and telephone number."*
- *"If I feel compelled to give my telephone number to a company selling me a product, I will give them my business number rather than my home number."*
- *„I do not participate in surveys that reveal my identity and inquire about the products and services I use."*
- *"I do not use store credit cards."*
- *"I do not join buying clubs such as the 'frequent buyers' club, the 'rewards card' club, or the 'book buyers' club."*

- *"I have 'Caller ID,' a system that may allow me to identify the number of the person making a telephone call to me."*
- *"I do not purchase items by mail."*
- *"When I receive a telephone call from an annoying telemarketer, I tell the caller to put my name on the company's 'don't call' list."*
- *"When buying items in a store, I make a special effort to pay by cash rather than to use a credit card or personal check."*
- *"I do not purchase items by telephone."*
- *"I have an unlisted telephone number."*
- *"When purchasing an item by mail or telephone, I request that information about me and my purchases not be shared with other companies."*
- *„I have telephoned or written to companies to have them remove my name from their calling or mailing lists."*
- *"Through my local telephone company, I have a 'blocking service,' which prevents my number from being transmitted to companies that use 'Caller ID.'"*
- *„If I feel compelled to give a telephone number to a company selling me a product, I will give them a fake number rather than my real number."*
- *"I have asked my credit card company(ies) to not disclose information about my buying patterns to any other companies."*
- *"I have asked the Direct Marketing Association (DMA) to have my telephone number removed from companies' calling lists."*
- *"I have asked the Direct Marketing Association (DMA) to have my name removed from companies' mailing lists."*
- *"My telephone answering machine warns the caller that I do not want to be bothered by telephone solicitors."*
- *„I have hired or asked a 'Privacy Advocate' to have my name deleted from mailing and telephone lists."*
- *„My telephone rings with one tone when a friend is calling me and with a different tone when someone else is calling me."*

Finally, the fourth section asked respondents to provide demographic data, like gender, age, race, and income. With the help of the questions of sections 2 and 3, three scales were built by testing reliability. Multiple regression analysis was used to correlate scales with demographic data in order to test the hypotheses.

As a result of section one, which includes questions about attitudes toward different direct marketing activities, the survey found that consumers dislike telemarketing (nearly to 100%) and direct marketing via mail. The most positive rating was given to catalogues as a marketing activity. The survey found that consumers' knowledge about direct marketing practice is very low (the average gave only three of ten correct answers). This finding fits neatly the results of other surveys. However, when faced with the increasing awareness and media coverage of privacy issues, the finding remains disturbing. The authors provide an interesting explanation: The awareness

focus on privacy violation on the Internet deflects from the traditional forms of direct marketing. Two consistent scales were developed and evaluated (summarizing results of instrument's section three). The awareness scale indicated that consumers have a relatively high awareness degree of most protection strategies from direct marketing activities. The protection scale indicated that, despite the high awareness level, consumers' usage of protection strategies against different marketing activities is low. According to findings, an explanation is that "consumers must perceive that the benefits from the strategy will exceed the costs of finding, initiating, and using it" (Dommeyer and Gross 2003, 48). Furthermore, the survey showed that "those who least desire direct marketing solicitations will be most motivated to adopt privacy protection strategies" (Dommeyer and Gross 2003, 48). This finding raises questions about privacy protection implementation and, in general, about consumers' motivations. The survey found that mediating factors such as age and gender do not play a big role in determining consumers' awareness and consumers' usage of protection strategies towards direct marketing activities.

Smith, Milburg, and Burke (1996) provide as a result of a study a validated measure instrument that can be used for further informational privacy research. Their study provides "two major contributions to the privacy literature: (1) a framework describing the primary dimensions of individuals' concerns about organizational information privacy practices and (2) a validated instrument for measuring those concerns" (Smith, Milburg, and Burke 1996, 188). The developed survey instrument contains a 15-item questionnaire that includes four subscales. Questions can be answered on a seven-point Likert scale from "strongly disagree" (1) to "strongly agree" (7). In order to develop the instrument three steps were undertaken by the scholars in the U.S.A. from 1989 to 1993 (Smith, Milburg, and Burke 1996, 175; 177-178). The final questionnaire is shown below (Smith, Milburg, and Burke 1996):

Here are some statements about personal information. From the standpoint of personal privacy, please indicate the extent to which you, as an individual, agree or disagree with each statement by circling the appropriate number.

- *A. It usually bothers me when companies ask me for personal information.*
- *B. All the personal information in computer databases should be double-checked for accuracy – no matter how much this costs.*
- *C. Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.*
- *D. Companies should devote more time and effort to preventing unauthorized access to personal information.*
- *E. When companies ask me for personal information, I sometimes think twice before providing it.*
- *F. Companies should take more steps to make sure that the personal information in their files is accurate.*

- *G. When people give personal information to a company for some reason, the company should never use the information for any other reason.*
- *H. Companies should have better procedures to correct errors in personal information.*
- *I. Computer databases that contain personal information should be protected from unauthorized access – no matter how much it costs.*
- *J. It bothers me to give personal information to so many companies.*
- *K. Companies should never sell the personal information in their computer databases to other companies.*
- *L. Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.*
- *M. Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.*
- *N. Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.*
- *O. I'm concerned that companies are collecting too much personal information about me.*

Items A, E, J, and 0 comprise the "Collection" subscale; items B, F, H, and L comprise the "Errors" subscale; items C, G, K, and M comprise the "Unauthorized Secondary Use" subscale; and items D, I, and N comprise the "Improper Access" subscale. Subscale scores are calculated by averaging the responses to the items for each subscale; an overall score is then calculated by averaging the subscale scores.

Campbell's research wants to contribute to a perfect partnership between business and customer, even if "consumers and business do not share a common set of values or understanding about privacy" (Campbell 1997, 45). She conducted a survey to explore both consumers' and managers' concerns about privacy in 1997. The notion of privacy, upon which the survey is based, refers to Alan F. Westin: "Information privacy is defined as the ability of individuals to determine the nature and extent of information about them which is being communicated to others" (Campbell 1997, 46). The survey was conducted in Canada's largest city, Toronto: First, 105 (weighed between male and female, average age between 24 and 34, average income level, majority had a university degree) randomly selected shopping mall visitors were interviewed with the help of a structured questionnaire.

The instrument included 15 pre-validated statements about personal privacy, which are identical to those used by Smith, Milburg, and Burke (1996) (reported within this document; see above).

In addition, several items were developed to explore respondents' prior use and knowledge of/experience with direct marketing. Knowledge about corporate practices was measured by using the following questions (a 7-point agree/disagree scale was used) (Campbell 1997, 56):

- *"How knowledgeable do you feel you are about how companies are collecting and using personal information?"*
- *"How knowledgeable do you feel you are about the benefits you receive from marketers' ability to use their information?"*

Personal direct and indirect experience with information misuse was measured (Campbell 1997, 56) (answer scale not available):

- *"How often have you personally been the victim of what you felt was an improper invasion of privacy?"*
- *"How much have you heard or read during the last year about the use and potential misuse of computerized information about consumers?"*

Also likelihood of placing an order using the telephone or direct mail was measured (Campbell 1997, 56):

- *"How likely would you be to place an order for products or services using the telephone?" (7-point agree/disagree scale)*
- *"How likely would you be to place an order for products or services using direct mail?" (7-point agree/disagree scale)*
- *"How many orders have you placed from any of the catalogs/pamphlets/booklets that you have received within the past year?" (5 categories: From "none" to "more than 20")*
- *"How recently have you placed an order from any of the catalogs/pamphlets/booklets hat you have received?" (6-point scale running from "never" to "within the last month")*

Second, 12 structured interviews with managers (involved in privacy issues) of companies using database marketing were conducted (open-ended questions about: a) their personal views on consumer information privacy, b) their assessment of collection, errors, and secondary use of consumer data, c) the mechanism used by their companies to adhere to personal privacy principles offered by the Canadian Direct Marketing Association, and d) their opinion on the necessity of governmental privacy protection.

Collected data was analyzed in different manners in order to address three research questions (RG) (Campbell 1997, 45):

- RG 1 "How do consumers feel about the collection and potential for errors and misuse of personal information?" (one-way ANOVA analysis was used)
- RG 2 "What individual variables are related to different aspects of consumers' information privacy concerns?" (correlation analysis was used)
- RG 3 "Do managers and consumers share the same views on information privacy concerns?" (comparison with the structured interviews).

Here are some of the research results:

- RG1: People indicated that they are highly concerned regarding privacy invasion. The factor analysis of the items of the used instrument (Smith, Milburg, and Burke 1996) resulted in three factors (unauthorized access/secondary use, collection, and errors) of personal information. Other than Smith, Milburg, and Burke (1996), unauthorized access and secondary use were not differentiated. Statistical results showed that people were more concerned about unauthorized access and secondary use of personal information than just gathering information.
- RG2: Correlation analysis showed a positive correlation between direct negative personal experience and consumer concerns about collection and errors. The analysis did not show a positive correlation between direct negative experience and consumers concerns about unauthorized access and secondary use of personal information. However, a positive correlation could be identified between indirect experiences (via the media) and concerns about unauthorized access and secondary use of personal information. Knowledge of corporate direct marketing practices had no effect on any of the information privacy concerns. Survey results suggested that it might be possible that less educated consumers are more concerned with secondary use of information/unauthorized access than higher educated consumers.
- RG3: The survey found a discrepancy between consumer and managerial views about informational privacy. Most managers identified targeting as the main issue of personal information (not privacy as the consumers do); they held the view that precise targeting generates benefits for the consumers. Many managers felt that an "opt out" by consumers' already fulfils privacy demands, so companies' activities should not refer to all advices outlined by the Canadian Direct Marketing Association. Managers valued the problems of unauthorized access, collection, errors, and secondary use of personal information in terms of profit gaining and competition.

Phelps, Nowak, and Ferrell (2000) conducted a quantitative survey, which aimed at assisting "public policymakers and marketers identify specific information practices and situations that foster consumer privacy concerns" (Phelps, Nowak, and Ferrell 2000, 27). In doing so, the authors were aware of the complexity of consumer privacy measurements. They identified several input factors, namely the type of personal information requested by marketers, the amount of information control offered, and the potential consequences and benefits expected (Phelps, Nowak, and Ferrell 2000, 31). These input factors would determine the outcomes, namely the beliefs regarding marketers' information practices and the overall concern level regarding the ways companies use personal information. As a consequence, these two categories (inputs and outcomes) would determine future outcomes, such as purchase likelihood and support for privacy measures. The U.S. wide survey was conducted via mail in June and August 1995. Two waves, each consisting of 500 polled people (N = 1000), were

conducted. Sample one included known and recent catalogue shoppers and sample two included randomly selected U.S. residents.

The survey found that the majority of the respondents were negative towards the privacy attitudes of direct mailing companies, felt that these companies knew too much about the consumers, disagreed with sharing or selling mailing lists of customers with other companies, and agreed that there should be limits to companies' collection of personal data. The analysis also showed that there was a strong relationship between the privacy concern level and beliefs in the importance of information protection. Overall results of the survey were that a) the type of information requested is crucial for privacy concerns; b) control over personal information including the control of dissemination is desired. Respondents indicated that they want the opportunity of self-regulatory practices. c) Most consumers link the dissemination of personal information with increased volume of advertising mail, and d) irrelevant advertising is the major contributor of consumers' privacy concerns.

In a 1992 survey, Nowak and Phelps differentiated between ignorance-based consumer concerns and knowledge-based consumer concerns (Nowak and Phelps 1992, 30). They were interested in the latter and worked based on research questions:

- about consumers' general concerns about personal privacy,
- about how concerned consumer are about direct marketing activities,
- about what specific types of information consumers are most protective of, and
- about what can be done about these concerns.
- In addition, the study was interested in exploring the relationship of privacy and ethics.

In order to answer these questions, the authors conducted an exploratory quantitative survey. A five-set telephone questionnaire was developed and 266 randomly selected adults (aged 18 years or older) were interviewed in a medium-sized Southeastern United States metropolitan area (approximately 150,000 people lived in the survey region; N was not representative of U.S. consumers; results are meant to be suggestive).

In the first set, consumers' general privacy concerns were assessed. In order to do so, distinctive ethical and privacy issues were presented and respondents were asked to rate these items on a 10-point importance scale. "The issues (the order of which was rotated during the actual administration) included: protecting freedom of speech; making sure women have equal rights; protecting rights to personal privacy; defending freedom of the press; and cleaning up the environment" (Nowak and Phelps 1992, 31).

In addition, two items were retrieved from the 1990 Harris/Equifax survey (answer opportunities on a 5-point scale: agree "very strongly", "somewhat strongly", disagree "somewhat strongly", "very strongly", "neither or not sure") (Nowak and Phelps 1992, 35):

- *"Consumers have lost all control over how personal information about them is used and circulated by companies".*
- *"Consumers are being asked to provide excessive amounts of personal information".*

The second set of survey questions measured consumers' knowledge about potential sources of information available for direct marketing. Some of the sources were legally accessible; some were not (according to the prevailing legal norms in the U.S.). "Here, consumers were read a list of 15 potential sources (with the order rotated across respondents) of information and asked to indicate whether it was 'definitely true,' 'probably true,' 'probably false,' or 'definitely false' that marketers or advertisers could purchase or rent the information contained in the source" (Nowak and Phelps 1992, 35).

The third set of questions examined consumers' concerns about the availability of specific types of personal information. A list was provided, which included information relating to purchase behaviour, personal information (such as age religion, income etc.), and media habits. Respondents were asked to rate for each item on a 4 point scale how upset they would feel, if the information were used by companies. In addition, concerns about specific information practices were analyzed. Therefore, scenarios of information gathering or information use practices were presented. Respondents were asked to rate for each scenario on a 4-point scale how serious an invasion of privacy they considered it to be. Respondents were also asked to rate based on a 4 point scale whether the scenarios were morally good or bad (Nowak and Phelps 1992, 33):

- *"A magazine publisher sells its list of subscribers so other companies can sell you goods or services".*
- *"A business calls you at home and tries to sell you something".*
- *"Merchants writing a code on the back of a check to record your race or ethnic group".*
- *"Credit/charge card companies monitoring the balance in your bank account".*
- *"The U.S. Postal Service rents or sells your address to direct mail companies and other businesses".*
- *"A company uses an automatic telephone number identification system (without your knowledge) to identify your phone number and address when you call them".*
- *"Companies collecting personal information about you for one purpose and then renting that information to other companies to use for different purposes".*

The fourth set of survey questions included items used for assessing consumers' beliefs about alternative practices of information gathering and information use. Re-

spondents could express their agreement on 5-point scale: agree "very strongly", "somewhat strongly", disagree "somewhat strongly", "very strongly", "neither or not sure") (Nowak and Phelps 1992, 34):

- *"It's acceptable for direct marketers to buy or sell the names and addresses of consumers without their knowledge."*
- *„Consumer privacy rights are adequately protected today by law and business practices."*
- *"Government should limit amount and type of consumer information that can tie collected."*
- *"There should be a federal commission or system to protect consumers' privacy."*
- *„Companies should have to get written permission from consumers before they sell or rent personal information."*
- *„The federal government should do more to protect the privacy rights of consumers."*

The survey showed that the general level of privacy concerns of respondents was similar to the results of the 1990 Harris/Equifax survey. Overall, respondents valued privacy and felt that privacy tends to be ever more violated. In Nowak and Phelps' survey, 82 % had concerns about threats to personal privacy (31 % were "very concerned", 51 % were "somewhat concerned"). 51 % said they had refused to give information to a company, because they thought it was unnecessary or too personal. 39 % of the respondents said that they had asked a company to remove their name and address from a mailing list. About 75% agreed that "consumers have lost all control over how personal information about them is used and circulated by companies". 64% of the respondents agreed that consumers are being asked to provide excessive amounts of personal information. Contrary to the generally high levels of privacy concern, the amount of information had been heard or read about the use or misuse of customer information was much smaller (only 37% said they had heard or read a lot about the potential use or misuse of computerized consumer data, 60 % indicated that they had heard or read very little).

A large percentage of consumers believed that marketers could use many different sources of information, even those that are not legally available (such as personal information collected in financial transactions, federal income tax forms, and medical records). However, many respondents were not aware that much of the personal information gathered by government is accessible to marketers (Nowak and Phelps 1992, 38). Most consumers believed that it is neither correct nor accurate that companies (and governments) store information. Nearly half of the respondents had heard about different "opt out" opportunities.

The study showed that consumers tend to have clear sentiments regarding types of personal information that are made available to marketers and advertisers: Respondents felt most upset by surveillance that makes data traceable to the individual as well as by the use of financial data for advertising purposes. Respondents indicated a

low concern for data about media habits purchase behaviours. Consumers were also considerably concerned about secondary information use (80% believed that collecting information for one purpose and then selling this information to other companies is an invasion of personal privacy; however, the concern was strongly related to consumers' expectations regarding a specific organization) and surreptitious data collection methods. Respondents wished to be more empowered and informed about such practices (they indicated that they desire transparency about whether their personal information is sold or collected; furthermore they indicated that they want to control these processes by themselves). In addition, consumers were "indeed more likely to construe information gathering and use practices as 'unethical' than as privacy invading" (Nowak and Phelps 1992, 36). "The finding that over half the respondents perceive direct marketing practices to be unethical implies 'privacy' is either a poorly defined construct or is masking consumers' true concerns" (Nowak and Phelps 1992, 38).

A quantitative survey conducted in 1993 was designed to "probe deeper into consumers' attitudes about database marketing activities" (Wang and Petrison 1993, 9) by Wang and Petrison. The study hypothesized that 1) "consumers may object more strongly to certain types of activities than to others" (Wang and Petrison 1993, 9), 2) "consumers may be more accepting of potential privacy infringements when they are conducted by certain kinds of companies" (Wang and Petrison 1993, 9), and 3) "some types of consumers might object more to privacy infringements in general than do others" (Wang and Petrison 1993, 9).

The survey was conducted in the area of Chicago, USA, among 1027 (N) randomly selected (random-digit dialling technology) English-speaking adults. It was carried out by the North-western University Survey Laboratory.

The survey questionnaire consisted of 114 questions. However, only two of them were privacy-related questions. The instrument was evaluated regarding its understandability and meaningfulness in a pilot test across a sample of 50 respondents. Interviews were conducted via telephone. Respondents were randomly split into two groups and were questioned with the help of two separate versions of the survey. Group one-respondents were asked (Wang and Petrison 1993, 10-11):

- *"Imagine that a company you do business with, such as a credit card company, keeps a record of your purchases and payment history and other information about you, and based on these records the company sends you information about products from other companies. How would you feel if this were to occur"?*

In addition, this group was asked (Wang and Petrison 1993, 11):

- *"Imagine you are overweight. A local hospital determines this by checking your height and weight on your driver's license records . . . and they send you information about their nutrition seminars and healthy heart seminars. How would you feel?"*

The second group was asked to answer to a different set of questions (Wang and Petrison 1993, 10):

- *"Imagine that a company you do business with, such as a credit card company, sells your name, address, purchase and payment history and other information about you to other companies, and based on these records the other companies send you information about their products. How would you feel?"*
- *"Imagine you are overweight. A local large-size clothing store determines this by checking your height and weight on your driver's license records . and they send you Information about their clothing. How would you feel?"*

Respondents were asked to place their attitudes on a 7 point scale that ran from "you would feel displeased", "you would feel nether displeased or pleased" to "you would feel pleased".

Group one's results for the first question showed that 22% of the respondents were at least somewhat pleased, 33% were neutral, and 46% were at least somewhat displeased. According to question two, results of the same group showed that 34% of the respondents were at least somewhat pleased, 21% were neutral, and 44% were at least somewhat unpleased. In comparison with the results of group two, consumers rate the companies' own use of personal information more positively than the companies' selling of information to third parties (10% of respondents were at least somewhat pleased, 16% were neutral, and 73% were at least somewhat unpleased). A comparison showed that consumers rate the hospital's use of data more positively than the clothing store's use of personal information (15% of the respondents were at least somewhat pleased, 18% were neutral, and 66% were at least somewhat unpleased). Research hypotheses one and two were supported. In order to verify hypothesis three, one had to find out if consumer attitudes correlated with personal characteristics. The survey found that people, who were concerned about their personal privacy, were more likely to be suburban dwellers and to have a higher income. People with health problems were more likely to want to be contacted by hospitals. A factor analysis of the results provided 12 factors as major underlying lifestyles, such as "retired people", "middle-age mainstreams", or "yuppies". The factors were correlated with privacy concerns in different manners, so that the survey showed differences among consumers concerning privacy.

In their survey, Milne and Rohm (2000) examined consumer awareness of data collection and consumer knowledge of name removal mechanisms, such as "opt out" and "opt in" across different direct marketing channels. Knowledge of name removal mechanism was interpreted as control of information. This interpretation is based on a control theory of privacy. Awareness is a logical precondition of control. The study

setting determined that only if both, awareness of data collection and knowledge of control mechanisms, is given, privacy exists. In 2000, the survey was conducted among 1508 randomly selected U.S. respondents, that were known to have purchased via direct mail. A questionnaire was used as survey instrument.

Deduced from the theoretical considerations about privacy, the survey tested the following hypothesis:

- "H1: Consumers are less likely to desire name removal from direct response lists when they are in an environment in which privacy exists than when they are in an environment in which privacy does not exist" (Milne and Rohm 2000, 240)
- Assumed that trust in the data collector and expected consumer benefit increase the willingness to trade privacy, the survey tested the following hypothesis:
- "H2: Consumers' desire to remove their names from direct response lists is negatively related to the consumer's direct response purchase experience" (Milne and Rohm 2000, 241).

In addition, the influence of several demographic data, namely the influence of computer use, age, affluence, education, political ideology, and gender was examined. Finally, the influence of the technological channel (e-mail or telephone) of direct marketing on the removal of names from marketing lists and the preferred format as well as the preferred frequency of name removal notices were tested.

Consumers were asked about their awareness of data collection by identifying types of information that were actually or could potentially be collected by companies (such as address, telephone number, and credit card information) (Milne and Rohm 2000, 243):

- *"What type of information do you think organizations with which you have done business have about you?" (binary answer opportunities regarding their names and addresses, telephone numbers, credit card information, and purchase history were provided)*

There was no true/false test of given answers. Instead, "respondents who indicated that organizations had three or four of the four types of information were classified as aware, and respondents who indicated two or fewer types were classified as not aware" (Milne and Rohm 2000, 243).

Nearly all consumers were aware that their address and telephone number were stored by organizations. Fewer indicated awareness of credit card information and that their purchase history was stored.

Consumers were asked about their knowledge of name removal mechanisms by indicating if they knew any ways to remove their name from direct marketing lists (Milne and Rohm 2000, 243). Respondents could answer "yes", "no", and "don't know".

Only 41,8% of respondents were knowledgeable of name removal mechanisms; others were not. Within the study framework, these facts mean that only 34% of all respondents had privacy. Hypothesis one and two were partially supported. Respondents were more likely to remove their names from telephone lists than e-mail lists. Respondents were more likely to remove their names from e-mail lists than from mail lists.

In general, the survey showed that privacy-aware consumers are less likely to remove their names from direct marketing, than others. The survey results showed that computer usage, age, affluence, and political ideology influence the desire to remove respondents' names from direct marketing lists. No effects were found for sex and gender. Respondents indicated that their preferred format of name removal were an easy-to-use "opt-out" opportunity (41% of respondents indicated this) or variant types of "opt-in" opportunities. In addition, respondents wished to be informed about these opportunities more frequently.

One of the rare qualitative studies examining privacy and surveillance was conducted by Ellis, Harper, and Tucker (2010) in 2010. The study focused on people's everyday experience with surveillance technologies (STs) and should elucidate "dynamic and contextual factors influencing people's accounts of their views and conduct in relation to STs" (Ellis, Harper, and Tucker 2010, 2). The researchers interviewed 31 members of London's public. The collected qualitative data show that people tend to imagine and fear a form of panoptic surveillance. This result contradicts newer theories within surveillance studies, which have moved beyond an Orwellian and panoptic notion of a centralized power of surveillance (Haggerty and Ericson 2000; Haggerty 2006) towards assuming that there is now a diversity of surveillance actors. Scholars explain that the contradiction between theory and people's perception stems from the psychological assumption that "order is possible a better prospect for ontological security … than chaos" (Ellis, Harper, and Tucker 2010, 4). In addition, the survey finds support for the extreme variability of privacy and surveillance concerns depending on different contexts or situations and the influence of trust. Furthermore, interviewees indicated that what they define as private sphere is varying: for some, the saying "my home is my castle", for others, the own body define the private sphere.

In contrast to Ellis, Harper, and Tucker (2010), John Gilliom (2001) undertook a qualitative research not among unspecified randomly selected people, but rather among a sample of surveillance victims, namely the welfare poor, who are under

permanent surveillance of state bureaucracy. Within this study, 48 women, mostly "heads of households in a region with little in the way of support, infrastructure, or economic opportunity" (Gilliom 2001, 44), were interviewed in Southeastern Ohio, U.S.A. The survey should "convey the women's vernacular terms and informal thoughts on these topics" (Gilliom 2001, 5), and should explore surveillance in a context of everyday life and casual talk. The data was collected using in-depth semi-structured interviews (Gilliom 2001, 151-152):

- *"NOTE: This is meant to be a guideline not an exact script. Make sure you avoid cuing the interviewee about law, privacy, or rights; but other than that feel free to use wordings that are most comfortable to you.*
  CONSENT FORM: Tell them what's up, explain the form, have them sign it before beginning.
  DEMOGRAPHICS: Age range, family size, time spent on welfare, types of programs used, county of residence.
  ICEBREAKER: Why did you go on welfare? (Try to get the story)"

- *"When you first applied for assistance, bow did you feel about the welfare office's requests for documentation of rent, utilities, birth certificates, and Social Security Cards?*
  Why do you think the welfare office wants so much information and documentation?
  Do you think the welfare agency would be able to find out if you did not report that you took a job in another county? Or had saving's in a bank in another state? Or received unemployment or disability payments? (How or why not for each.)
  Have you, yourself, ever kept things from your caseworker or bent the truth about income, family size, work history in order to improve your benefits? Any unreported cash income? If not, why not? If so, did you get caught?
  What about other folks you know, what sorts of things do people do to make ends meet?
  How do you feel about people who don't fully report their income or resources? (Why?)
  Do you talk with other welfare clients and share information about rules, caseworkers, or different programs? Did you ever get or give any advice on how to apply for programs or report information?"

- *"A few years ago, the welfare system started using a new statewide computer called CRIS- E. In general, has your service and delivery of benefits gotten better or worse with the new computer? (For post-computer clients, simply ask how their service has been with the new computer.) (How? Examples? How else? Any complaints?)*
  Can you tell me what sorts of information the computer has about you and your family? (Fully probe awareness of their own data file, number matching and other types of verification; don't cue them at this point; just use vague questions.) What else? What else? What else?

We've talked a fair bit about how computers have changed the way welfare works, but I now want to give you some more information about the new system. The welfare office is able to do what are called computer number matches, where they use the Social Security numbers of people in your family to look and see if you have money or income that you're not reporting. They use information from state and federal taxes, Social Security information, statewide wage records, and information from unemployment compensation, workman's comp., and state retirement systems. They make a computer check of this information several times a year and your caseworker gets all of this information.
Were you aware of this?
How do you feel about it? (Push them to talk and explain.)
Have you ever gotten any letters or had to see your caseworker because of something that turned up in a wage match or some other way? (If so, what happened, how was it resolved?)
Do you think it will prevent fraud and cheating?
How do you think people will work around it?
Does it bother you when they do so much checking up on you? Why or why not? (Push them to talk and explain.)
In some states, the welfare agency fingerprints their clients to make sure they are who they say they are. How do you fell about that? Why?"

- *"Debrief: Has this interview raised any questions that you would like to ask me, or made you think of things that you would like to bring up?"*

- *"If you are left with any questions or concerns, you may want to talk with your caseworker or their supervisor, or you may want to consult with legal services, which can provide you with free legal advice about problems or questions you have about your benefits. (Provide phone numbers for local offices.)"*

The interviews were conducted by local interviewers, who had firsthand knowledge of welfare surveillance problems and have been former victims. Interviewees were instructed to tell their story of how they ended up going on public assistance, and how well they are "getting by" with that assistance. Interviewees' knowledge of welfare surveillance and how they feel about these activities was inquired. After that, people were informed of the welfare bureaucracy's actual capacities to surveil, "and how such a [bureaucracy] system would affect the different types of income enhancement that clients engaged in" (Gilliom 2001, 47). Interpretative results of the survey showed that common theories and political arguments of the "right to privacy-discourse" do not meet the empirical reality, problems, and needs of people being kept under surveillance: "The mothers complained about the hassle and degradation caused by surveillance and the ways that it hindered their ability to meet the needs of their families. They advanced few claims tied to the right of privacy; instead, they told particular stories about daily need and about the power of surveillance to both make

their needs greater and limit their capacity to meet them. They made references not to the great claim of due process, but to their own struggles to cope and to the power of surveillance to thwart them. In their need and anger, they mounted no litigation or protest campaigns, but engaged in necessarily quiet practices of everyday resistance and evasion to beat, as best they could, the powers of surveillance" (Gilliom 2001, 6).

2.2. Empirical Research on Online Privacy

In the following sub-section, existing empirical research on online privacy is analysed. A discussion of some of the most cited studies should give a representative overview of typical empirical research approaches that assess privacy on the Internet. However, for a well-balanced overview some studies grounded in critical theory are examined as well. The studies and any important findings are briefly summarized in order to assess the strength as well as possible pitfalls and shortcomings of the existing empirical research.

Andrade, Kaltcheva and Weitz (2002) examined in an exploratory study how companies can influence consumers' concerns about self-disclosure of personal data on the Internet. They assume that consumers' willingness to disclose personal information is based on their assessments of the costs and benefits. Companies can alter this cost-benefit trade-off by, on the one hand, increasing the subjective benefits, or, on the other hand, reducing the subjective costs of self-disclosure. They identified three different approaches:

- developing a reputation for trustworthiness,
- provide a comprehensive privacy policy indicating how the disclosed information will be used, and
- offering rewards (e.g. coupons, gifts) for disclosing the information.

Among 114 undergraduate students from a large Southeastern university, Andrade, Kaltcheva and Weitz carried out a paper- and-pencil questionnaire, containing both quantitative as well as qualitative elements. For example, participants had to express their feelings about the following statement: "Simply register with us and tell us a little more about yourself. You will receive a $10 check. Don't miss this opportunity".

Participants were shown two different privacy policies, which they were asked to evaluate with three seven-point semantic-differential scales: detailed vs. not detailed, complete vs. incomplete, and informative vs. uninformative. Likewise the reputation of companies was assessed with three seven-point semantic-differential items: good vs. bad, trustworthy vs. untrustworthy, and good reputation vs. bad reputation.

The results indicate that privacy policies as well as a high reputation of the company reduce the level of privacy concern, whereas any offer of reward increases it.

Nearly one third (31%) even indicated receiving a reward as being ”suspicious“. Still, the authors highlight, that this surprising finding may vary according to the type of information solicited and the type of reward offered by the company. Worth mentioning seems the extremely low amount of respondents (4%) that indicated that they entertain suspicion with respect to privacy policies.

Awad and Krishnan (2006) conducted a survey in order to examine the relationship between information transparency and consumer willingness to partake in personalization. They pursued the following two research questions: ”Do information transparency features, which provide knowledge of information and procedures, affect consumer willingness to be profiled online for personalized offerings? Does the effect of information transparency features on a consumer's willingness to be profiled online differ across personalized service versus personalized advertising?“ (Awad and Krishnan 2006, 14).

Information transparency features allow consumers to access the information a firm has collected about them, and how that information is going to be used, e.g. data transparency, data removal, and time expirations of data (Awad and Krishnan 2006, 14). In their survey, Awad and Krishnan explicitly contrasted if the collected information was used for personalized advertising or for providing personalized services. Their study was based on a fresh analysis of data from a survey already conducted at a large Internet service provider during summer and fall 1998. 523 participants completed the survey. They were selected from a group of readers of the ”Family PC“ magazine. This sample differed from the national average in so far as they showed a higher level of education, Internet usage, and household income.

With the help of a 3-point Likert-scale, respondents were asked to assess the following statements (Awad and Krishnan 2006, 22):

- *“Importance of whether a site is going to use the information they collect from me in a way that will identify me.”*
- *“Importance of know how long a company will retain information they collect from me in their database.”*
- *“Importance of knowing what information a company keeps about me in their databases.”*
- *“Importance of why, for what purpose, the company is collecting info from me.”*
- *“Concern about threats to your personal privacy in America today.”*
- *“Concern about threats to your personal privacy today when using the Internet.”*

The findings of the study support the hypothesis that consumers who value information transparency features are less willing to be profiled online. The authors therefore suggest ”that firms adopt a strategy of providing features that address the needs

of consumers who are more willing to partake in personalization, therefore accepting that the privacy sensitive minority of consumers are unwilling to participate in personalization, despite additional privacy features“ (Awad and Krishnan 2006, 13). Such strategy may exclude privacy sensitive consumers from services and special offers.

Interestingly, the study suggests that consumers perceive the value of online services to be greater than online advertising. Another notable finding is that the study shows that privacy policies do not have significant value to consumers. Though consumers may rate a privacy policy as important, few of them actually take note of the policy when using the site (Awad and Krishnan 2006, 25).

Bellman, Johnson and Kobrin (2004) investigated whether concerns about privacy can be explained by differences in cultural values, privacy regulation and Internet experience. Their concern was that ”differences in culture and national regulation create challenges for global information management strategies, sometimes limiting or even preventing the free flow of valuable information“ (Bellman, Johnson and Kobrin 2004, 313). They used a global sample of 534 online consumers from 38 countries. Less than half of the participants (37%) were female, the mean age was 32 years, and the average education level was between ”some college“ and ”college graduate“ (only 23% were fulltime students). The survey consisted of 15 items (seven point Likert scales: strongly disagree – strongly agree, complemented by a no opinion-option, in order to not force responses), clustered in 4 groups: collection, unauthorized secondary use, improper access and errors. Example questions (Bellman, Johnson and Kobrin 2004, 317) in these categories are the following:

- *”When Web sites ask me for personal information, I sometimes think twice before providing it.“ (Collection),*
- *”Databases that contain personal information should be protected from illegal access – no matter how much it costs“ (Improper access).*
- *”Web sites should devote more time and effort to verifying the accuracy of the personal information in their databases“ (Errors).*
- *“When people give personal information to a Web site for some reason, the Web site should never use the information for any other reason.“ (unauthorized secondary use).*

The research shows that most privacy concerns of consumers ”are highly related to the privacy regulatory framework prevailing in a particular country, which tends to reflect as well as shape the privacy preference of individual consumers“ (Bellman, Johnson and Kobrin 2004, 322). However cultural influence could only be seen in two dimensions: errors in databases and unauthorized secondary use, rather than in the overall concern for information privacy. The authors drew the following managerial implication from this finding: ”although consumers from all the countries in our sam-

ple feel the same level of overall concern about information privacy, consumers from countries with no privacy regulation or with omnibus regulation desire more government involvement in the regulation of corporate privacy practices than consumers from countries with sectoral privacy regulation. Since regulatory structure largely mediates cultural influences, managers generally need only know the regulatory regime that applies in a country to adequately adjust their privacy policies to the privacy preferences of consumers in that country." (Bellman, Johnson and Kobrin 2004, 322).

Some interesting, more detailed findings are that participants with more Internet experience were less concerned about online privacy overall, older participants were more concerned about privacy overall, and females indicated more concern on the subscale of secondary use of data.

Buchanan, Paine, Joinson and Reips (2007) introduced a scale for identifying and quantifying people's privacy concerns, which was established in context of three short Internet-administered surveys measuring privacy-related attitudes (Privacy Concern) and behaviours (General Caution and Technical Protection). In the first study, 515 people completed an 82-item questionnaire, from which the scales for the three above mentioned surveys were derived. Questions relating to different aspects of privacy were included (Buchanan et al. 2007, 159):

- *Informational privacy: "Are you concerned that you are asked for too much personal information when you register or make online purchases?"*
- *Accessibility: "Are you concerned that information about you could be found on an old computer?"*
- *Physical Privacy: "Are you concerned about people viewing your screen over your shoulder when you are online?"*
- *Expressive Privacy: "Are you concerned that an e-mail you send someone may be inappropriately forwarded to others?"*
- *Further questions aimed at measuring perceived benefits of surrendering privacy, privacy-related attitudes and behaviour (Buchanan et al. 2007, 159):*
- *"How acceptable is it that personal information provided online can be used to speed up log in/purchases?" (benefits)*
- *"How acceptable is it that law enforcement agencies track users of Web sites to track criminals?" (benefits)*
- *"Do you clear your Internet browser history regularly?" (behaviour)*
- *"Are you concerned about who might access your medical records electronically?" (attitude)*

In the second survey, the scale validity was examined by comparing scores from groups considered likely to differ in privacy-protective behaviours. 69 students from

the Open University (UK), partly from technology-based studies (38 participants) and partly from social sciences (31 participants), answered a Web-based questionnaire with a refined set of 16 privacy attitude items and 12 privacy behaviour items, as shown in the tables (Buchanan et al. 2007, 161-162):

General Caution

1. Do you shred/burn your personal documents when you are disposing them?
2. Do you hide your bank card PIN number when using cash machines/making purchases?
3. Do you only register for websites that have a privacy policy?
4. Do you read a website's privacy policy before you register your information?
5. Do you look for a privacy certification on a website before you register your in-formation?
6. Do you read license agreements fully before you agree to them?

Technical Protection

1. Do you watch for ways to control what people send you online (such as check boxes that allow you to opt-in or opt-out of certain offers)?
2. Do you remove cookies?
3. Do you use a pop up window blocker?
4. Do you check your computer for spy ware?
5. Do you clear your browser history regularly?
6. Do you block messages/emails from someone you do not want to hear from?

Table 15: Privacy Behaviour Items (source: Buchanan et al. 2007, 161)

Privacy Concern

1. In general, how concerned are you about your privacy while you are using the Internet?
2. Are you concerned about online organisations not being who they claim they are?
3. Are you concerned that you are asked for too much personal information when you register or make online purchases?
4. Are you concerned about online identity theft?
5. Are you concerned about people online not being who they say they are?
6. Are you concerned that information about you could be found on an old computer?
7. Are you concerned who might access your medical records electronically?
8. Are you concerned about people you do not know obtaining personal information about you from your online activities?
9. Are you concerned that if you use your credit card to buy something on the Internet your credit card number will obtained/intercepted by someone else?
10. Are you concerned that if you use your credit card to buy something on the Internet your

card will be mischarged?
11. Are you concerned that an email you send may be read by someone else besides the person you sent it to?
12. Are you concerned that an email you send someone may be inappropriately forwarded to others?
13. Are you concerned that an email you send someone may be printed out in a place where others could see it?
14. Are you concerned that a computer virus could send out emails in your name?
15. Are you concerned about emails you receive not being from whom they say they are?
16. Are you concerned that an email containing a seemingly legitimate Internet address may be fraudulent?

Table 16: Privacy Concern Items (source: Buchanan et al. 2007, 162)

Overall the technical and non-technical students did not differ significantly in their level of online privacy concern, but did so on the technical protection scale, as well as on the general caution scale.

In the third survey (which in general was concerned with people's attitudes towards identity cards within the UK), correlations between the scores of the developed scales and two already established measures of privacy concern (Westin-Harris and the Internet- IUIPC) were examined. 1,122 participants took part in this third survey, which showed significant and positive correlation with the other two already established scales. The authors of the survey criticized existing studies for solely focusing on informational privacy as well as the used privacy scales for being one-dimensional constructs. Such studies "do not separate out all of the different factors that could be considered privacy issues" (Buchanan et al. 2007, 158). Based on a multi-faceted understanding of privacy as for example put forth by DeCew (1997), they argue for scales "attempting to measure concern should tap these different facets about which people may be concerned" (Buchanan et al. 2007, 158). However, the presupposed multifactorial nature of privacy concerns could not be isolated into its various dimensions. Buchanan et al. argue that "given the substantive conceptual overlap between many of the dimensions, it may be somewhat naïve to expect to be able to develop pure measures of each" (Buchanan et al. 2007, 164).

The authors also aimed at measuring positive attitudes towards giving up privacy in some cases, such as providing information in order to process online transactions, but failed to do so. One reason for the non-emergence of positive attitudes might be that "the framing of the questionnaire inadvertently introduced a biased response set. The questionnaire instructions referred to concerns people might have, and most of the items also refer to concerns about or the acceptability of various things. It might be more appropriate for possible benefits of online information sharing to be assessed using a separate questionnaire, with instructions and phrasing less likely to induce a distrustful response set." (Buchanan et al. 2007, 164). Furthermore they

tried to not only ask for attitudes, but as well as for privacy-related behaviours, thereby expanding existing privacy scales.

The authors conclude that the developed scales are reliable and valid instruments for use in online privacy research. Noticeable, Buchanan's et al. scales focus on privacy invasions by third/unauthorized persons, but neglect to account for economic privacy/surveillance as for example measuring attitudes towards targeted advertising.

Milne, Rohm and Bahl (2004) undertook three consumer surveys in order to examine consumer's propensity to protect themselves from online identity theft. They assess attitudinal, behavioural and demographic antecedents that predict the tendency to protect one's privacy and identity online. As most other studies, they identify the main threat posed on consumers in identity theft or fraud conducted by third/unauthorized persons, using cookies, hacking into hard drives, intercepting transactions or spyware. But they neglect possible threats imposed by behavioural targeting and overall economic surveillance. In particular Milne, Rohm and Bahl addressed the following research questions:

- "What is the relationship between offline data protection practices and online protection behavior?
- What is the relationship between online shopping behaviors and online protection behavior?
- What is the relationship between privacy attitudes and online protection behavior?
- What is the relationship between demographics and online protection behavior?" (Milne, Rohm and Bahl 2004, 218).

The first study was an online survey of 2,468 adults (and Internet users) residing in the US, randomly drawn from the multimillion Harris online panel. These data were utilized to measure the influence of attitudinal and behavioural antecedents on online privacy protection. Two additional surveys were conducted to supplement the data and investigate any relationship between online and offline identity theft protection behaviour. These additional studies were identical and consisted of a 6-page survey, representing 300 college students from a large university located in the north-eastern U.S. The other survey represents 40 nonstudent responses.

Part of the questions were designed as true-false statements. For example (Milne, Rohm and Bahl 2004, 221):

- *"I clear my computer's memory after browsing."*
- *"When given the chance, I opt-out of third party information sharing."*

- *"I always look for and read privacy policies on the Web."*
- *"In addition to my work e-mail, I have a separate e-mail account for my personal e-mail."*
- *"I talk with my children about getting my permission before giving out information online."*
- *"I make sure that online forms are secure before filling out information."*
- *"I set up my browser to reject unnecessary cookies."*
- *"I use anonymous remailers."*
- *"I encrypt my e-mail."*
- *"I use anonymizers while browsing."*

Another set of questions asked the respondents whether they had done any of the following. For example (Milne, Rohm and Bahl 2004, 222):

- *"Refused to give information to a Web site because you felt it too personal or unnecessary."*
- *"Asked a Web site to remove your name and address from any*
- *lists used for marketing purposes."*
- *"Asked a Web site not to share your name or personal information with other companies."*
- *"Decided not to use a Web site or purchase something from a Web site because you were not sure how your personal information would be used."*
- *"Set your computer to reject cookies."*
- *"Supplied false or fictitious information to a Web site when asked to register."*

The results indicate that nonstudents are more likely to protect themselves than students, whereas – non-surprisingly – the students, usually being more technically savvy, scored higher at more advanced privacy protection actions such as using anonymizers while browsing or anonymous re-mailers. Consistent with other surveys, only less than a majority (in survey 2 only 22%, in survey 3 46%) looked at and read the privacy policy. Additionally the surveys found that less than a majority use technology for protecting their personal information. In survey 1 a significant correlation between general attitudes and behaviours toward privacy and online privacy protection behaviour was found. Online privacy protection was more common with male participants, who have more years of schooling and are of a younger age. The authors indicate that "much work in educating and motivating consumer to follow recommended protective measures needs to be done", as well as "training in how to use technical tools" for self protection (Milne, Rohm and Bahl 2004, 230).

In their survey, Miyazaki and Fernandez (2001) tried to examine the implications of consumers' perceived risks of e-commerce. They used a pencil and paper survey, which was structured into mainly two parts. First, Internet experience was assessed

by examining the duration of experience as well as the frequency of Internet use. Second, respondents' online purchase behaviour and their concerns regarding online shopping were evaluated. Data was collected by trained data collectors, who approached potential respondents in randomly assigned areas of the major international airport of a large U.S. city (population over 1 million). The final sample was 160, with respondents aged from 15 to 75 (mean of 34,5), almost equally balanced gender (52% male/ 48% female), a median of four year degree education and a household gross income of $6-70.000.

Respondents' concerns pertaining to online shopping were assessed with the following item:

- *"Whether or not you have made purchases over the Internet, what concerns do you have about making purchases over the Internet?" (Miyazaki and Fernandez 2001, 33)*

Respondents provided a total of 269 concerns, which were then classified into six general categories: 1) Privacy-Infringement by Online Retailers 2) System Security - Third Party Fraudulent Behaviour 3) Security – Fraudulent Behaviour of Online Retailers 4) Inconveniences of Online Shopping 5) No concerns and 6) Miscellaneous (nonsense and uncategorized responses).

Overall the study shows that higher Internet experience as well as the use of other remote purchasing methods (e.g. mail-order or tele-shopping) is related to lower levels of perceived risk toward online shopping. In turn, this results in higher online purchase rates. The authors underline that "the content analysis of the open-ended concerns regarding online shopping shows that consumers have a keen interest in both privacy and security issues" (Miyazaki and Fernandez 2001, 38). Interestingly, they found that though System Security concerns were the top concern, "privacy was actually a greater concern for consumers with longer periods of experience, suggesting that the accumulation of such experience (and, presumably, information) may lead to higher concerns regarding privacy issues. This is in direct contrast to suggestions that more experience leads to fewer privacy concerns and is an issue that calls for additional research" (Miyazaki and Fernandez 2001, 38). Miyazaki and Fernandez conclude by suggesting that "although the acquisition of consumer information may yield short-run advantages, perceived breaches in privacy and security likely will hinder online retailing in the long run, due either to consumer distrust or legislative mandate. In that increased Internet experience alone does not appear to diminish privacy concerns, it is evident that safe and responsible handling of consumer information will be a strategic tool for the promotion of online retailing." (Miyazaki and Fernandez 2001, 39).

In an e-mail survey of online users, Sheehan (2002) examined whether online privacy concerns mirror the offline environment. The study aimed to explore online privacy concerns and attempts to categorize online consumers according to Westin's typology. Two specific research questions were asked:

- "Can online users be segmented into distinct groups based on Westin's typology of privacy concern?
- If so, are there differences in these groups based on demographics and/or their computer usage" (Sheehan 2002, 22)?

The study was conducted in the very early days of private Web usage (November 1997 – February 1998). An e-mail survey was sent to 3724 individuals by generating e-mail addresses by a directory search engine. With 889 completes surveys a 24% response rate was reached. The sample consisted of about 70% men, with more than 60% earning a bachelor's degree or higher and a higher than average household income. By using 15 statements reflecting five categories of privacy influence, the following privacy concerns were assessed:

- awareness of data collection,
- information use,
- information sensitivity,
- familiarity with entity,
- compensation.

For each influence three situations were presented, different in regard to their average degree of privacy concern (low, moderate, high). The statements were shown in random order and rated on a 7-point bipolar scale (not at all concerned – highly concerned).

Additionally the frequency of different behaviours was measured using a 1-7 scale (never take action – always take action). The situations and behaviours presented and measured in the survey are shown in the following table (Sheehan 2002, 25):

Situations (predicted level of concern)

(Concern with privacy in each situation measured using a 1–7 scale where 1 D not at all concerned and 7 D extremely concerned.)

Awareness

You receive e-mail from a company you have sent e-mail to in the past (low concern)
You receive e-mail from a company whose web page you recently visited (moderate concern)
You receive an e-mail and have no idea how the company got your address (high concern)

Usage

A company requests your e-mail address only to send information of interest (low concern)
A notice on a web page states that information collected is used by other divisions of that company (moderate concern)

A notice on a web page states that information collected on that web page may be sold to other companies (high concern)

Sensitivity
You are asked to provide your name to access home page (low concern)
You are asked to provide names of newsgroups read to access home page (moderate concern)
You are asked to provide your Social Security Number to access home page (high concern)

Familiarity
You receive e-mail about a new product from a company you currently do business with (low concern)
You receive e-mail about a new product from known company you don't do business with (moderate concern)
You receive e-mail about a new product from a company you've never heard of (high concern)

Compensation
A web page requires your e-mail address to access the page; upon registration, you will be entered in a contest to win a computer (value: $1000) (low concern)
A web page requires your e-mail address to access the page; upon registration, you will receive a 25% discount on future purchases (moderate concern)
A web page requires your e-mail address to access the page; upon registration, you will receive a mouse pad (high concern)

Behaviors
(Frequency of adopting behavior measured using a 1–7 scale where 1 D never take action and 7 D always take action)

Reading unsolicited e-mail.
Registering (i.e., providing information about oneself) for web sites
Providing inaccurate information when registering for web sites
Providing incomplete information when registering for web sites
Notifying Internet service providers about unsolicited e-mail
Requesting removal from e-mail lists
Sending highly negative messages to entities sending unsolicited e-mail (e.g., "flaming")

Table 17: Survey statements for assessing privacy concern and behaviours (source: Sheehan 2002, 25)

The findings show that the vast majority of the users could be labelled "pragmatic". In contrast to Westin's results (25% fundamentalists, 25% unconcerned, 50% pragmatists), over 80% of respondents comprise the pragmatist category. As a result the author broadened the typology to take into consideration more of the contextual aspects of the Internet. The pragmatist category was split up into segments of more and less concerned individuals. The four groups have been termed (1) unconcerned Internet users, (2) circumspect Internet users, (3) wary Internet users and (4) alarmed Internet users. There are no significant differences among the four groups in terms of gender and household income, but in terms of age and education. Persons with higher levels of education are more concerned about their online privacy. Persons over the age of 45 tended to be either not at all or even highly concerned about their privacy. The study's author suggests that the alarmed Internet user category may be underreported, due to the sensitive nature of privacy online. Highly concerned individual

might not have answered the survey. According to Sheehan (2002, 31), this type of bias is present in all studies of privacy.

Also interesting in this context is the national survey of Internet privacy and institutional trust by Turow and Hennessy (2007). In 2003, they undertook 1200 quantitative telephone interviews in the United States with adults (18 years and older), who go online at home (Turow and Hennessy 2007, 304). The authors tried to analyse whether US citizens trust political and economic institutions regarding the protection of online privacy.

The survey questionnaire contained among demographic and online activity patterns also questions about individual behaviour, attitudes, and regulation policies related to Internet privacy. For instance, the participants were asked if they:

- *"Argued with a family member about personal or family information that the person released to a chatroom or on email" (2.2% said yes);*
- *"Had an incident where you worried about something a family member told a website" (1.7% said yes);*
- *"Chose not to register on a website because it asked you for personal information to get into the site" (34.6%);*
- *"Talked with a family member about how to deal with requests for information from websites" (12.4%); and*
- *"Searched for instructions on how to protect information about yourself on the web" (5.9%) (Turow and Hennessy 2007, 305).*

In addition, the interviewees were asked whether they had provided the following information on websites:

- *"Give mail address" (12.3%);*
- *"Give email address" (19.2%);*
- *"Give real name" (33%); and*
- *"Give age" (47.8%) (Turow and Hennessy 2007, 305).*

The respondents were also asked if they:

- *"Used software that looks for spyware on your computer" (22.8%);*
- *"Used software that hides your computer's identity from websites that you visit" (17.8%);*
- *"Used a filter program to block unwanted emails" (44.4%); and*
- *"Erased all or some of the unwanted cookies on your computer" (67.9%) (Turow and Hennessy 2007, 305).*

In order to analyse concerns about absence of control over personal information on the web, Turow and Hennessy (2007, 305) asked participants to indicate to which

degree they agreed with the following statements (five-point Likert scale from strongly agree to strongly disagree):

- *"I am more concerned about giving away sensitive information online than about giving away sensitive information any other way";*
- *"I should have a legal right to know everything that a website knows about me";*
- *"My concern about outsiders learning sensitive information about me and my family has increased since we've gone online";*
- *"I look to see if a website has a privacy policy before answering any questions';*
- *'Teenagers should have to get their parent's consent before giving out information online";*
- *"I sometime worry that members of my family give information they shouldn't about our family to web sites"; and*
- *"I am nervous about websites having information about me".*

In order to study respondents' general trust and belief in economic actors respect of online privacy, they were confronted with statements like the following ones (five-point Likert scale from strongly agree to strongly disagree):

- *"I trust websites not to share information with other companies or advertisers when they say they won't"; and*
- *"When a website has a privacy policy, I know that the site will not share my information with other websites or companies" (Turow and Hennessy 2007, 305).*

The authors also tried to measure participants' understanding of the efficiency of different forms of possible privacy regulations. The items were:

- *"A law that requires website privacy policies to have easy-to-understand rules and the same format";*
- *"A law that requires companies that collect personal information online to help pay for courses that teach internet users how to protect their privacy online"; and*
- *"A law that gives you the right to control how websites use and share the information they collect about you" (Turow and Hennessy 2007, 306).*

Furthermore, in order to study negative expressions of institutional trust, the interviewees were asked:

- *"On a scale of 1 to 5, with 5 being the most important and 1 being the least important, how likely will 'Your internet service provider', or 'Banks or credit card companies', or 'Major advertisers', or 'Microsoft Corporation', or 'Privacy protection software companies' or 'The government' be to release or share information about you by accident or on purpose without your knowledge or consent?" (Turow and Hennessy 2007, 306).*

Turow and Hennessy (2007, 309) conclude "that with the exception of major advertisers [40% of respondents distrust; TA], straight trust or distrust is not the mode

when it comes to information privacy. Between one-third and half of the respondents simply sit on the fence, not believing that they can trust or distrust an institutional actor when it comes to privacy. Even more interesting is the substantial percentage of strongly conflicted people between one-third and one-quarter are conflicted about how these key institutions of the digital world relate to their privacy. They seem to feel that while institutional actors will help them to control their information online, those same actors (or others parts of them) will take that information privacy away".

In 2005, Turow, Hennessy, and Bleakley (2008) conducted 1500 quantitative telephone interviews with adult Internet users (18 years and older) in the United States in order to analyse people's knowledge of entrepreneurial rights to collect personal information on- and offline.

In order to measure people's knowledge of privacy rights, the interviewees were asked whether the following statements are true or false:

- *"Companies today have the ability to follow my activity across many sites on the Web";*
- *"A Web site is allowed to share information about me with affiliates without telling me the names of the affiliates";*
- *"When I subscribe to a magazine, by law that magazine cannot sell my name to another company unless I give it permission";*
- *"My supermarket is allowed to sell other companies information about what I buy";*
- *"When I give money to charity, by law that charity cannot sell my name to another charity unless I give it permission";*
- *"A video store is not allowed to sell information about the titles I have rented"; and*
- *"When a Web site has a privacy policy, it means the site will not share my information with other Web sites or companies" (Turow, Hennessy, and Bleakley 2008, 416).*

Knowledge Items with Correct Answers and Survey Percentage Correct (N = 1500)

Knowledge Items o Collecting and Disclosing Personal Data	**Correct Response**	**% Correct**
Companies today have the ability to follow my activity across many sites on the Web.	True	83
A Web site is allowed to share information about me with affiliates without telling me the names of the affiliates.	True	51
When I subscribe to a magazine, by law that magazine cannot sell my name to another company unless I give it permission.	False	48
My supermarket is allowed to sell other companies information about what I buy.	True	36
When I give money to charity, by law that charity cannot sell my name to another charity unless I give it permission.	False	28

A video store is not allowed to sell information about the titles I have rented.	True	29
When a Web site has a privacy policy, it means the site will not share my information with other Web sites or companies.	False	25

Table 18: People's knowledge of entrepreneurial rights to collect personal information on- and off-line (source: Turow, Hennessy, and Bleakley 2008, 416)

More than 80 per cent of the respondents were aware that companies are able to follow people's activities online, but only a half of the survey participants knew that an online company is allowed to share users' information with affiliates without telling users the affiliates' name. Also interesting is that three-quarters of the interviewees think that a web site operator will not share users' information with other web sites or companies if the web site has a privacy policy.

Based on these findings, Turow, Hennessy, and Bleakley conclude: "Our conclusion is that a small proportion of Internet-using American adults have a highly sophisticated knowledge framework regarding marketplace privacy. That segment has learned the regulations that allow it to correctly distinguish the circumstances in which merchants have the right to share information in different marketplace domains. A slightly larger proportion (the ones who knew all but the video-store answer) holds a less sophisticated, but nevertheless typically correct, framework. From our data, we cannot tell whether this framework reflects actual knowledge of every specific marketplace domain except for video stores or whether it is based on a general assumption (wrong only in the video-store case) that the government always allows merchants to share people's private information. It is clear from the data that the large majority of Internet-using adults understand that regulations regarding merchants' sharing information are domain specific. At the same time, that majority was only sporadically correct regarding the true-false statements. The general picture of the population at large is one of the selective and limited knowledge about where in the marketplace one might find merchants who are legally allowed to share customers' personal information without their consent (2008, 419f)".

In summary, the economic realm seems to be the most prominent in empirical online privacy studies. On the one hand, the Internet in itself is a space, shaped by economic interests, on the other hand, economic actors operating on the Internet are highly interested in consumer's attitudes and behaviour in order to improve their consumer experience and further capitalize on them. Therefore, economic organisation may be heavily engaged in funding costly empirical research. However, except for Turow and Hennessy (2007) and Turow, Hennessy, and Bleakley (2008) none of the above listed studies critically assess privacy in the economic realm.

2.3. Empirical Research on Web 2.0/Social Media/Social Networking Sites (SNS) Privacy and Surveillance

The task of this sub-section is to give a representative, but still eclectic overview about different studies of privacy and surveillance on web 2.0.

Studies of privacy and surveillance on web 2.0 primarily focus on privacy-related issues on corporate social networking sites such as Facebook and MySpace. These studies pay attention to one ore more of the following issues concerning SNS users:

- Individual knowledge and information towards/about privacy.
- Individual privacy-related attitudes/concerns.
- Individual behaviour and practices towards/about privacy (settings).

Acquisti and Gross (2006, 37) conducted an online survey of students, staff and faculty members (N=294; 147 male and 147 female participants) at a US academic institution in order to study their privacy concerns as well as their usage, knowledge and attitudes towards Facebook (FB). The questionnaire contained around forty questions including an initial set of screening questions, a set of calibration questions, a consent section, and questions relating to Facebook (Acquisti and Gross 2006, 39). In the questionnaire, the participants were asked to rank agreement, concern, worries, or importance on a 7-point Likert scale (where 1 is "not important at all" and 7 is "very important"); the questions ranged from general ones, to more and more specific, and personal ones (Acquisti and Gross 2006, 43).

According to Acquisti and Gross (2006, 47), "members claim that the FB is very useful to them for learning about and finding classmates (4.93 mean on a 7-point Likert scale) and for making it more convenient for people to get in touch with them (4.92), but deny any usefulness for other activities". Among the stated reasons for using Facebook, having fun and revealing useful information were ranked top (Acquisti and Gross 2006, 53). The study stresses that the users' knowledge about privacy issues on Facebook is very low: "30% claim not to know whether FB grants any way to manage who can search for and find their profile, or think that they are given no such control. Eighteen percent do not know whether FB grants any way to manage who can actually read their profile, or think that they are given no such control. … 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." (Acquisti and Gross 2006, 51-52) In addition, "almost 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).

The survey furthermore shows that although privacy concerns may drive older and senior university members away from Facebook, primarily undergraduate students joining the network regardless of their privacy concerns (Acquisti and Gross 2006, 47). To a certain extent, privacy attitudes determine who joins Facebook, but once joined, there is only little difference in information disclosure across different social groups (Acquisti and Gross 2006, 50).

Fogel and Nehmad (2009) carried out a quantitative survey with students at a University in New York City (N=205; equal percentages of men and women; average age: 22 years). The study analyses risk taking, trust, and privacy concerns among students in the context of social networking sites (Facebook and MySpace). Participants were asked at the university campus to complete an anonymous questionnaire with questions such as:

- *"Do you read a website's privacy policy before you register you [sic] information?" (5-point scale from 1=never to 5=always) and*
- *"I am concerned that the information I submit on the Internet could be misused" (1=strongly disagree to 5=strongly agree) (Fogel and Nehmad 2009, 155).*

In the survey, more than three-quarter of the students had registered at a social networking site and nearly three-quarter of the participants allowed to view their profile without restrictions (Fogel and Nehmad 2009, 156-157). "In conclusion, those who have profiles on social networking websites have greater risk taking attitudes than those who do not have profiles on social networking websites. Also, risk taking attitudes are greater among men than women. Facebook has a perception of being a trustworthy social networking website. General privacy concerns and identity information disclosure concerns are of greater concern to woman than men. Lastly, there are greater percentages of disclosure of phone numbers and home addresses among men than women." (Fogel and Nehmad 2009, 160)

boyd and Hargittai (2010) conducted a quantitative paper–pencil survey with 1115 participating students in 2009 at the University of Illinois, Chicago, and followed up with the same group using a quantitative paper survey sent by postal mail in 2010 (495 valid completed survey responses). The study examines the attitudes and practices of 18- and 19-year-old students about privacy settings on Facebook. The survey addresses the following questions:

- *"During a year in which Facebook altered its privacy settings accompanied by widespread media attention, to what extent did the site's users alter their settings?";*
- *"How does frequency of Facebook use relate to whether or not people adjust their privacy settings?";*
- *"How does confidence in managing privacy settings correlate with the practice of doing so?";*

- *"Is gender correlated with either confidence in or the practice of managing privacy settings?"; and*
- *"Is general Internet user skill related to either confidence in or the practice of managing privacy settings?" (boyd and Hargittai 2010).*

boyd and Hargittai (2010) asked participants to indicate to which degree they agreed with the following statement: "I feel confident changing the privacy settings of my Facebook account" ("strongly disagree" to "strongly agree"). In addition, the respondents were asked how often they change their Facebook privacy settings ("never", "have done it once", "have done it 2–3 times", and "have done it 4 or more time").

87% of the respondents were members of Facebook in 2009 and 90% joined the network in 2010. boyd and Hargittai (2010) found that "while not universal, modifications to privacy settings have increased during a year in which Facebook's approach to privacy was hotly contested. We also find that both frequency and type of Facebook use as well as Internet skill are correlated with making modifications to privacy settings. In contrast, we observe few gender differences in how young adults approach their Facebook privacy settings, which is notable given that gender differences exist in so many other domains online".

Furthermore, the data showed that "far from being nonchalant and unconcerned about privacy matters, the majority of young adult users of Facebook are engaged with managing their privacy settings on the site at least to some extent. The frequency with which they adjust their settings and their confidence in doing so may vary, but most report modifying their settings" (boyd and Hargittai 2010).

Christofides, Muise, and Desmarais (2009) undertook a quantitative online survey with 343 participating undergraduate students (261 women, 81 men; age: 17 to 24) at a university in Ontario, Canada. The survey endeavoured to analyse information disclosure and information control on Facebook and wanted to explain the personality factors that effect levels of disclosure and control. In detail, the authors were interested to receive answers to what information students disclose, how they control access to that information, and personality factors (need for popularity, trust, self-esteem, and general tendency to disclose, need for popularity, general tendency to disclose personal information, levels of trust, and likelihood of disclosing personal information) related with online information control and disclosure (Christofides, Muise, and Desmarais 2009, 342).

The questionnaire contained demographic questions, questions about information disclosure, likelihood of using available privacy settings on Facebook, and types of posted pictures. In the questionnaire, the participants were for example asked:

- *"How likely are you to say no to a Facebook friend's request in order to control who has access to your information?" (7-item scale) (Christofides, Muise, and Desmarais 2009, 342).*

Students disclose more personal information on Facebook than they disclose in general (Christofides, Muise, and Desmarais 2009, 342). In addition, "participants were very likely to have posted information such as their birthday and e-mail address, and almost all had joined an online network. They were also very likely to post pictures such as a profile picture, pictures with friends, and even pictures at parties and drinking with friends" (Christofides, Muise, and Desmarais 2009, 341).

The authors also found out that "information disclosure and information control were not significantly negatively correlated, and multiple regression analyses revealed that while disclosure was significantly predicted by the need for popularity, levels of trust and self- esteem predicted information control. Therefore, disclosure and control on Facebook are not as closely related as expected but rather are different processes that are affected by different aspects of personality" (Christofides, Muise, and Desmarais 2009, 341).

Debatin et al. (2009) realized an online quantitative (N=119) and qualitative (N=8; open-ended in-depth face-to-face interviews) empirical research with undergraduate students at a US academic institution. The study strives to analyse the relationship between Facebook privacy issues, privacy settings, recognized benefits and risks on Facebook, as well as restrictions of privacy.

The study was based on the following research questions:

- "How important is Facebook to its users and which role does it play in their social life?";
- "To what extent is Facebook part of everyday rituals or has created its own rituals?";
- "Which role does Facebook play in creating and promoting gossip and rumors?"; and
- "Which negative effects, particularly with respect to privacy intrusions, does Facebook have?" (Debatin et al. 2009, 90).

The online questionnaire contained 36 multiple-choice questions classified into thematic groups such as Facebook habits, types of personal information available on the users' profile, users' practices with regard to privacy, role of friends in Facebook use, potential risks of Facebook, negative incidents, difference between perceived negative incidents to oneself and to others, and demographic variables. For example, in order to study users' practices with regard to privacy, the participants were asked:

- *"if they were familiar with Facebook privacy settings" (yes/no);*

- *"if they protected their profile" (yes/no); and*
- *"how they protected their profile" (survey options mirrored actual Facebook options: 'I'm not sure,' 'All of my networks and all of my friends can see it,' 'some of my networks and some of my friends can see it,' 'only my friends can see it,' and 'I have different settings for different parts of my profile')" (Debatin et al. 2009, 91).*

From the online survey respondent pool, eight students (six female, two male) were asked for open-ended in-depth face-to-face interviews. The eight interviewees were selected according to their survey answers and their availability. After recording and transcribing the interviews, the data was analysed based on a combination of typological reduction analysis, qualitative content analysis, and hermeneutical/rhetorical interpretation. In order to identify and interpret relevant statements, the authors' used following categories: invasion of privacy, breach of trust, gossip and rumours, violation of boundaries, and habitual or ritualized use of Facebook (Debatin et al. 2009, 92).

One result of the study was: "While the majority of Facebook users report having an understanding of privacy settings and make use of their privacy settings, it is also apparent, however, that they may have a skewed sense of what that exactly entails. Additionally, as hypothesized, perceived benefits of online social networking outweighed risks of disclosing personal information. Risks to privacy were ascribed more to others than to the self. If Facebook users reported an invasion of personal privacy, users are more likely to change privacy settings than if they reported hearing of an invasion of privacy happening to others" (Debatin et al. 2009, 100).

The authors furthermore stress that "the interviews exemplified how deeply Facebook is integrated into daily routines and rituals, and how much it has produced its own routines and rites. The habitual use of Facebook and its integration into daily life indicates that it has become an indispensable tool of social capital and connectedness with large numbers of people. The benefits of Facebook outweigh privacy concerns, even when concrete privacy invasion was experienced" (Debatin et al. 2009, 100).

Although Ellison, Steinfield, and Lampe (2007) focused in their survey on the relationship between the usage of Facebook and the maintenance of social status, the authors also analysed privacy concerns of individuals. Ellison, Steinfield, and Lampe carried out a quantitative online survey with undergraduate students (N=286) at the Michigan State University (MSU). Their instrument included four broad types of measures, namely measures of demographic variables (gender, age, local/home residence, ethnicity, year in school), measure of Internet usage, measure of Facebook usage (time spent on Facebook, reason for usage), and measure of individual well-being and social status. Ellison, Steinfield, and Lampe's (2007, 1165) findings can be summarized as follows: "We asked Facebook users whether or not they had set the privacy settings on their accounts to control who viewed their profiles. More than two

thirds (70%) either did not know (suggesting that they left the default setting of all members of the MSU network) or said that their profile was visible by the entire MSU network. Only 13% limited access only to their friends, while the rest blocked only certain individuals".

Hinduja and Patchin (2008) conducted a quantitative content analysis of MySpace. They collected and analysed types of information found on randomly sampled MySpace profile pages that were publicly accessible (N=1475; age: 16-17 years). In order to record certain kinds of information of MySpace profile pages, the researchers used a data collection form. The data collection form contained variables such as name, birth date, telephone number, postal address, last login date, evidence of alcohol, tobacco, or drug use, number of pictures, and swear words in profile (Hinduja and Patchin 2008, 141-142).

The authors summarized their findings as follows: "Almost 40% of the profiles included the youth's first name, and approximately 9% included their full name. This information, along with their current city (81%) and school (28%), may also assist those seeking to identify profile owners offline. While it is effortless to contact youth via their MySpace profiles (using private messages or public comments), some youth also included their instant messaging name (4%, usually a screen name for AOL, Yahoo, or MSN Messenger) or an additional email address (1%). In rare cases (n = 4) youth reported their personal (usually cell) phone number. In addition to the phone numbers reported within the profile by its owner, we noticed a few cases where friends would include their own phone numbers in a public comment they left… Four profiles out of approximately 1500 represents a small percentage (about one-third of 1%), however, this number extrapolated to all adolescents on MySpace suggests that up to 75,000 youth may be including this very private information" (Hinduja and Patchin 2008, 136).

Hinduja and Patchin (2008, 136) concluded that "this review of MySpace profiles also revealed that many adolescents seek to demonstrate familiarity with adult-oriented behaviors. For example, many youth indicated they had recently consumed alcohol (18%), while others noted that they had smoked cigarettes (8%) or used marijuana (2%)."

Lewis, Kaufman, and Christakis (2008) undertook an analysis of college students' privacy settings on Facebook and endeavoured to find out factors that are predictive of a student having a private or public profile. In order to reach full access to the student's profiles, the scholars created an undergraduate account and participated in the university network on Facebook (Lewis, Kaufman, and Christakis 2008, 84). The authors realized a quantitative content analysis of Facebook profiles of 1564 undergraduate students at a private university in the northeastern United States. The

dataset was extracted directly from Facebook and included variables such as sex, friends, hometown, race/ethnicity, socioeconomic status, and online activity.

The following hypotheses formed the core of the survey:

- "The more friends with private profiles a student has, the greater will be the student's likelihood of maintaining a private profile herself";
- "The more active a student is on Facebook, the greater will be the student's likelihood of maintaining a private profile";
- "Private profiles will be more common among women than among men"; and
- "Students with private profiles will exhibit a set of cultural preferences that is distinct from that of students with public profiles" (Lewis, Kaufman, and Christakis 2008, 82-83).

As a result of the study, Lewis, Kaufman, and Christakis (2008, 94-95) stress that privacy behaviour is a consequence of both social influences and personal interests and sum up: "A student is significantly more likely to have a private profile if (1) the student's friends, and especially roommates, have private profiles; (2) the student is more active on Facebook; (3) the student is female; and (4) the student generally prefers music that is relatively popular (high mean) and only music that is relatively popular (low SD)".

In the Greater London area, Livingstone (2008) conducted qualitative interviews with 16 teenagers (8 females, 8 males; age: 13-16 years), who use social networking sites such as Facebook and MySpace. Livingstone was interested in showing that online opportunities on the one hand and risks such as privacy threats on the other hand are interconnected and that both issues characterize social media. In the study, the interview schedule addressed three main topics, namely motivations and literacies forming the teenagers' profile, the semiotic understanding of others' profiles, and the social meanings of the contacts encouraged online and their connection to offline relations (Livingstone 2008, 398). After recording and transcribing the interviews, the data was coded based on participants' responses and the asked questions.

Although Livingstone (2008, 406) found out that teenagers see the maintenance of old and the establishment of new friendships as a central opportunity of social networking sites, she discovered that the interviewees were concerned about privacy settings on these sites: "A fair proportion of those interviewed hesitated to show how to change their privacy settings, often clicking on the wrong options before managing this task, and showing some nervousness about the unintended consequences of changing settings (both the risk of 'stranger danger' and parental approbation were referred to here, although they also told stories of viruses, crashed computers, unwanted advertising and unpleasant chain messages)". Livingstone (2008, 406) concluded: "when asked whether they would like to change anything about social net-

working, 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".

Dwyer, Hiltz, and Passerini (2007) and Dwyer et al. (2010) conducted quantitative online surveys with 115 MySpace and 107 Facebook users in the US, and 388 studiVZ (a German-based social networking site) users in the German-speaking world in order to study the influence of trust and privacy concerns on the use of social networking sites for social interaction. The questionnaire contained questions about general use of the site, perceptions of trust, Internet privacy concerns, information sharing, and the development of new relationships (Dwyer, Hiltz, and Passerini 2007).

The participants were asked to indicate to which extent they agreed with the following statements (for the studiVZ survey, the questions were translated into German):

- *"I prefer to send a message to a friend using [name of SNS] rather than through using email."*
- *Participants were asked to indicate which personal information they disclose in their profile (photograph, real name, hometown, e-mail address, cell phone number, relationship status, sexual orientation, and instant messenger screen name).*
- *"I find it easy to meet new people on [SNS]."*
- *"Members were also asked if they had initiated contact with a person they met on the social networking site using another communications method, such as face to face, e-mail, telephone, or instant messenger."*
- *"I believe most of the profiles I view on [SNS] are exaggerated to make the person look more appealing" ("strongly disagree" to "strongly agree")*
- *"I worry that I will be embarrassed by wrong information others post about me on [SNS]." ("strongly disagree" to "strongly agree") (Dwyer, Hiltz, and Passerini 2007)*
- *"I have adapted the privacy settings to control who can view my profile on [name of SNS]" ("strongly disagree" to "strongly agree")*
- *"In order to control who can contact me using [name of SNS] I have adjusted my privacy settings." ("strongly disagree" to "strongly agree")*
- *"I don't use the privacy settings to control who can access my profile." ("strongly disagree" to "strongly agree")*
- *"I never accept invitations of people I never met before." ("strongly disagree" to "strongly agree")*
- *"When I use [name of SNS] I ignore people whom I never heard of and who try to contact me." ("strongly disagree" to "strongly agree")*
- *"I don't use [name of SNS] to make contact with people whom I've never heard of." ("strongly disagree" to "strongly agree")*
- *"The original founders of [name of SNS] would view my use of the privacy settings as inappropriate." ("strongly disagree" to "strongly agree")*

- *"The founders of [name of SNS] would disagree with how I use the privacy settings." ("strongly disagree" to "strongly agree")*
- *"I am confident that I know how to control who is able to see my profile on [name of SNS]." ("strongly disagree" to "strongly agree") (Dwyer et al. 2010, 2974)*

The authors conclude "that Facebook members reveal more information, but MySpace members are more likely to extend online relationships beyond the bounds of the social networking site. Paradoxically, MySpace has stronger evidence of new relationship development, despite weaker trust results. Even MySpace subjects with high distrust in other members report strong levels of relationship development. The results suggest that for MySpace, trust is not as necessary in the building of new relationships as it is in face to face encounters" (Dwyer, Hiltz, and Passerini 2007).

In addition, the authors found out that there is a significant difference of privacy settings between the US based (Facebook and MySpace) and the German (studiVZ) social networking sites: "StudiVZ users are the most familiar with their privacy settings … StudiVZ users also generally feel confidence in their ability to modify their privacy settings … Members of StudiVZ express a higher level of familiarity … and facility … with their privacy settings, but express less comfort … with their abilities" (Dwyer 2010, 2975).

The analysis of existing research literature shows that empirical studies of privacy on web 2.0 mostly focus on privacy-related issues on commercial social networking sites such as Facebook and MySpace. These studies pay attention to issues of users on social networking sites, namely individual knowledge and information about privacy, individual privacy-related attitudes, and individual behaviour towards privacy.

3. A Discussion of Existing Empirical Research on (Online) Privacy and Surveillance

This section provides theoretical considerations (3.1), a critical inquiry (3.2), and some methodological implications (3.3) of empirical research on (online) privacy and surveillance.

3.1. Theoretical Aspects of Empirical Research on (Online) Privacy and Surveillance

Some theoretical considerations of what is missing within the existing empirical research on privacy and surveillance will now be provided. First, this is argued on a general level; then specific arguments for offline, online and web 2.0 research will be provided.

3.1.1. Empirical Research on Privacy and Surveillance (In General)

Many empirical studies focus on individual privacy concerns and individual privacy-related behaviour. What is missing is a critique of the political economy of privacy and surveillance that takes into account the larger societal context of privacy of surveillance.

The critique of political economy approach is based on a social understanding of human beings, who can only realize their full potential within society that is free of domination (Marx 1843; 1867). However, the classical paradigm of privacy dates back to the liberal tradition and the rise of capitalism (MacKinnon 1989; Habermas 1991, 74; Mill 1965, 232, 938; Fuchs 2011c). Within this theoretical tradition and social ordering, the individual has to be protected from social encroachments. So, classical notions of privacy (Warren and Brandeis 1890; Westin 1967, 7) are individualistic and see in the first instance surveillance as an individual threat (Lyon 1994, 196).

Privacy as control of information was the grounding notion of almost all reported surveys. For example, Milne and Rohm (2000) found that only 34% of all respondents were in a state of privacy, because privacy was defined as awareness of data collection and knowledge of consumers' control mechanisms regarding data collection. To define privacy only as control of personal information, no matter what qualities of information privacy should include, is problematic from a critical point of view because such an understanding of privacy advances the particularistic interests of commercial actors. Commercial interest groups want people to give up privacy in order to follow surveillance based business models such as targeted advertising and selling personal data to third parties. According to the control theory of privacy this is a legitimate process (Posner 1978/1984) because in this theory informational privacy is defined as self-determined information behaviour (Rachels 1975; Fried 1968).

A lot of research was conducted in order to clarify companies' opportunities to increase customers' perceived control of information within business models that depend on consumer surveillance. For example, Culnan and Armstrong (1999) found that fair information procedures that bring about an increased control over personal information, decrease privacy concerns of consumers. Within most of the surveys, this commercial interest is addressed by building up trust between customers and companies and by establishing fair interactions (Gandy 2003, 294-296).

Based on political economy analysis, one can conclude that a notion of privacy, which includes only control of information, serves as ideology because such a notion deflects from underlying economic domination structures, which are reproduced by capital accumulation via surveillance-based business models. Instead, a collective notion of privacy should be important for a critical empirical research interest. A collective notion of privacy has for example been formulated by Etzioni. He views pri-

vacy "as the realm in which an actor (a person or a group, such as a couple) can legitimately act without disclosure and accountability to others. Privacy thus is a societal license that exempts a category of acts (including thoughts and emotions) from communal, public, and governmental scrutiny" (Etzioni 1999, 196). So, collective notions of privacy try to establish societal commitment. Such notions usually are opposed to classical liberal theory, which presents privacy as a necessary shield from the public or the collective. In existing empirical studies, to some extent collective notions of privacy were used by analyzing respondents' concerns about privacy and surveillance legislation. Such questions go beyond the narrow notion of privacy as individuals' control of personal information.

Surveys show that the knowledge of privacy legislation is rather low in general. This applies especially for privacy legislation that affects the private sector (Chan et al. 2008, 12). Therefore, it may not make sense for a critical empirical study to simply ask people to give collective mandatory definitions of privacy, especially of economic privacy. Asking survey respondents or interviewees for a definition of privacy, is a research strategy that is too general and too far detached from everyday experiences. Instead, it may be promising to ask questions about different actually existing surveillance threats in order to draw implications if there respondents have a rather collective or individualistic understanding of privacy.

Besides the capitalist (or totalitarian) state (government, legislation) that is a promoter of surveillance (see for example Gilliom 2001), collective notions of privacy may be found in relation to people's common (class) interests or in their position within the process of production. Critical empirical research should explore whether people, based on common experiences, have an interest in a specific quality of privacy (which is not represented in existing legislations) or in freedom from surveillance or not and how such interests can look like. But collective notions of privacy should be seen critically as well: Several surveys found that consumers are most concerned about maintaining privacy of sensitive financial information. For example, Culnan (1993) reports that 71% of the respondents of a survey wanted that financial information should never be shared by organizations. Nowak and Phelps (1992) report similar results. It is likely that people want their financial information protected because otherwise it would affect their competitiveness on commodities markets. In competitive societies, privacy serves the ability to compete "and with preventing access to knowledge about me that can be of use to my competitors. Thus, if I am bidding against an economic rival, it might make a big difference to me whether I was able to keep the actual state of my finances [...] 'secret'" (Geuss 2001, 88). People are likely to see privacy that is related with private property, as an important moral value of society. If this is the case, then they would for example vote for laws protecting private property in order to protect their own financial privacy. From a critical political economy point of view, it becomes clear that such a private property-centred notion of privacy is highly problematic because it can reproduce and ideologically justify social inequality. In capitalism, the right to private property enables the appropri-

ation and accumulation of value that is produced by others (Marx 1844, 41; 1976, 732). Under such circumstances, financial privacy is an ideology because it protects the wealth of the rich and of companies by making their financial operations and possessions intransparent and invisible to the public. Additionally, it protects social inequality by making no differentiation between property of the worker, which is needed for economic survival, and property of the rich (for example means of production or access to the public sphere), which enables exploitation of the workers. It is not possible to question social inequality if data about this phenomenon remains hidden because it is protected by financial privacy rights.

The example shows that a collective notion of privacy should be combined with an analysis of capitalist society that includes the notion of exploitation and the critique of ideologies. Critical research should be interested in a collective notion of privacy, which is oriented on the common good and creating structures in society that benefit all, not just some or a few. This includes the human right to have freedom from domination and exploitation. This concept of privacy differs not only from the individualistic control theory of privacy, but also from other liberal notions of privacy, which are interested in defining a specific quality of the private that is mandatory among individuals (and that includes property, for example).

3.1.2. Empirical Research on Consumer Privacy and Surveillance (Offline and Online)

Within the existing empirical research literature on consumer privacy and surveillance on the offline and online level, there are few attempts to operationalize collective notions of privacy, a lot of uncritical consumer privacy research, and hardly attempts to explore economic privacy in a critical manner. The latter would mean to relate privacy to private property and competition. Mainly due to direct or mediated interests of commercial surveys, there is a predominance of uncritical economic (consumer) privacy research. This uncritical research does not challenge the origins of people's need to compete, capitalists' monetary benefits of consumer benefits, and structural power asymmetries between classes.

3.1.3. Empirical Research on Privacy and Surveillance on Web 2.0/Social Media

Many empirical studies focus on individual privacy concerns and individual privacy-related behaviour. Economic issues do not play an important role in these studies. In the context of web 2.0, some authors have advanced critique of this kind of studying privacy (Beer 2008; Fuchs 2009, 11-22; Fuchs 2010a, 2010b, 2011a) and contribute to filling the identified gap with critical arguments.

For Beer (2008), a more political analysis that focuses on the workings of capitalism is missing: "By focusing solely upon the user, … we are overlooking the soft-

ware 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 [social network(ing) sites; TA], 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. … So, when we ask about who are using SNS and for what purpose, we should not just think about those with profiles, we should also be thinking about capitalist interests, of third parties using the data, of the organising power of algorithms (Lash, 2007a), of the welfare issues of privacy made public, of the motives and agendas of those that construct these technologies in the common rhetoric of the day, and, finally, of the way that information is taken out of the system to inform about the users, or, in short, how SNS can be understood as archives of the everyday that represent vast and rich source of transactional data about a vast population of users" (Beer 2008, 523-526).

Fuchs (2009, 11-22; see also Fuchs 2010a, 2010b, 2011a) criticizes the existing approaches of studying privacy on Web 2.0 as uncritical and individualistic and says that they tend to overlook the greater societal context: "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. … It focuses on the analysis of individual usage behaviour without seeing and analysing 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. … 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. … 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 … The crucial point here is that no matter if users set their profiles to visible or invisible, commercial ISNS [Integrated Social Networking Sites; TA] 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" (Fuchs 2009, 13-22).

In addition, some authors conducted critical empirical case studies of economic surveillance and targeted advertising (Sandoval 2011; Fernback and Papacharissi 2007) and have thereby helped advancing a critique of the political economy of online/web 2.0 surveillance (Fuchs 2011b).

Sandoval (2011) conducted a content analysis of the terms of use and privacy statements of the 52 most popular web 2.0 platforms such as wikis, weblogs, social networking sites, and file sharing sites. She wanted to find out how "surveillance contribute to capital accumulation on web 2.0" and how "the owners of commercial web 2.0 sites collect and disseminate user information" (Sandoval 2011). The coding scheme used four main categories, namely general characteristics, advertising, data collection, and data dissemination (Sandoval 2011). From the 52 analysed web 2.0 platforms, 51 were privately owned and commercially organized (Sandoval 2011). In addition, the vast majority of web 2.0 platforms displayed advertisement (Sandoval 2011). "The terms of use and privacy statements of commercial web 2.0 platforms allow the widespread use of user data in a way that supports the profit interests of platform owners. The business model of most commercial web 2.0 platforms is based on personalized advertising. Capital is accumulated by selling space for advertisements as well as by selling user data to third-party advertising companies." (Sandoval 2011)

Fernback and Papacharissi (2007) conducted a discourse analysis of online privacy statements of four websites with web 2.0 applications, namely MSN, Google, Real.com, and Kazaa. The survey was undertaken in order to find out how these sites are able to deal with personal information of their users (Fernback and Papacharissi 2007, 722). The authors concluded: "The MSN use of language articulates a concern for Microsoft's legal standing rather than for consumer protection. The Google privacy statement offers consumers little protection. The Kazaa statement is dismissive of consumer concerns, and the Real statement is a contradictory promotional apparatus" (Fernback and Papacharissi 2007, 730). In addition, Fernback and Papacharissi (2007, 730) state that "each privacy statement initially assures consumers of a commitment to privacy and subsequently dismantles any true protection of consumer data. These portals are businesses and must be free to operate as such; they must be able to profit responsibly, without undue restriction. However, these privacy statements pose virtually no restriction on businesses to profit excessively from the collection and use of consumer information. … The rhetoric of these privacy statements reveals business practices that favor profit initiatives over consumer protection".

Based on terms of use and privacy policies, Fuchs (2011b) analysed an empirical sample of the most-used web 2.0 platforms in the USA regarding ownership and advertising rights. His findings show that the majority of popular web 2.0 platforms in the USA such as Facebook, YouTube, MySpace, Blogspot, and Flickr are corporate-based. With the help of legal instruments such as privacy policies and terms of use,

these platforms have the right to store, analyse, and sell personal data of their users to third parties for targeted advertising in order to accumulate profit (Fuchs 2011b). Fuchs (2011b) furthermore stresses that an asymmetric economic power relation characterizes web 2.0, because companies own the data of their users, while the users do not at all have ownership rights in these companies although they produce economic value for these companies and can be considered as unpaid and infinitely exploited labour force. The structure of web 2.0 primarily maximizes power of the dominating economic class that owns such platforms and benefits the few at the expense of the many (Fuchs 2011b). Fuchs (2011b) argues that it is important to study web 2.0 based on the approach of the critique of the political economy of media and communication by employing terms such as class, exploitation, and surplus value. The creation of profit on platforms like Google, Facebook, or MySpace is mainly achieved by the exploitation of the work of users of these platforms, who produce user-generated content that is commodified and sold to advertising clients, who target the users with ads that are individually customized with the help of surveillance procedures (Fuchs 2011b). "New media corporations do not (or hardly) pay the users for the production of content. One accumulation strategy is to give them free access to services and platforms, let them produce content, and to accumulate a large number of produsers that are sold as a commodity to third-party advertisers." (Fuchs 2011b) The productive labour time involves "all of the time that is spent online by the users" that is "produced completely for free" and characterizes "an essential part of the capitalist production process" (Fuchs 2011b). This means that users produce profit for large corporations during web 2.0 activities such as creating profiles and sharing ideas on Facebook, announcing personal messages on Twitter, uploading or watching videos on YouTube, and writing personal entries on Blogger. It is the "total commodification of human creativity" (Fuchs 2011b). On web 2.0, "producers are consumers and consumes producers of information. Therefore, producer surveillance and consumer surveillance merge into web 2.0 prosumer surveillance" (Fuchs 2011b).

Also some other authors have tried to situate the logic of web 2.0 surveillance in the context of exploitation, exchange value, free labour, social factory, netslaves, new strategies of capital accumulation, commodification, and post-Fordism (Andrejevic 2010; Terranova 2004; Cohen 2008; Coté and Pybus 2007; Petersen 2008; Scholz 2008).

Andrejevic (2010) wants to help developing a theory of exploitation on commercial social networking sites. "This chapter argues that more work need to be done to clarify the relationship between willing participation and commercial exploitation. What is needed is an explanation of how a theory of exploitation might apply to the conditions under which user-generated content creates value." (Andrejevic 2010, 83) For Andrejevic (2010, 94), "exploitation entails some form of coercion" and "obtains when there is loss of control over one's creative, productive activity". The users' activities on social networking sites are treated as free resources. Web 2.0 platforms

have the right to store, analyse, and sell personal data of their users to third parties for targeted advertising and "the use of this information will be shaped by existing power relations and structures of ownership" (Andrejevic 2010, 85). Terms of use and privacy policies of commercial social networking sites aim at asserting rights to store, analyse, and sell personal data of their users (Andrejevic 2010, 87). Web 2.0 activities such as creating profiles and sharing ideas, announcing personal messages, uploading or watching videos, and writing personal entries on commercial social networking sites have the capacity to produce value (Andrejevic 2010, 89). These activities are "both unpaid (outside of established labor markets) and freely given, endowed with a sense of autonomy" (Andrejevic 2010, 90). Andrejevic furthermore stresses that commercial social networking platforms strive to appear as open, interactive and participatory networks, where users are able to control their own activities. In fact, these promises "enlist the participatory public in the process of marketing to itself" (Andrejevic 2010, 95), influence the users' behaviour with the help of targeted marketing more effectively (Andrejevic 2010, 96), and overlook asymmetrical power relations and structures of ownership. Greater participation of web 2.0 users leads to greater and more exclusive forms of proprietary knowledge (Andrejevic 2010, 95). The users' "free participation is redoubled as a form of productive labor captured by capital. In a self-generating cycle, the offer to overcome estrangement or alienation produces a second-order form of separation: that of users form the data they generate" (Andrejevic 2010, 94). Andrejevic (2010, 96) describes commercial social networking sites as part of the "social factory". "In the social factory, the boundaries between spheres of labor and leisure, domesticity, and consumption upon which the distinction between consumer choice and workplace coercion relies, become blurred. To the extent that our communicative, educational, and social lives are folded into the social factory and become the resources that we draw upon and sell to employers, access to resources for online networking becomes a crucial component of generating value" (Andrejevic 2010, 97). Andrejevic (2010, 99) therefore argues for a not-for-profit online infrastructure, a non-commercial web 2.0, and a real networked interactivity. Andrejevic's notion of a theory of exploitation on commercial social networking sites can be summarized as follows: "This chapter's premise is that the new forms of communication, transaction, consumption, and interaction made possible by digital technologies need to be situated within their larger economic context, namely, the creation of a privately owned and operated commercial media structure. When we explore what people do on Facebook or MySpace and the forms of community such sites enable, we must also keep in mind what gets done with the products of this activity, who controls its use and re-use, who profits from its transformation into commercial commodities and marketing campaigns, as well as who is targeted by these campaigns and to what end. Contrary to conventional wisdom, social networking sites don't publicize community, the privatize it. Commercial social networking sites are ostensibly collaborative productions, except when it comes to structuring terms-of-use agreements, and, of course, allocating the profits they generate" (Andrejevic 2010, 97).

Terranova (2004, 73-74) speaks in the context of the digital economy about "net-slaves", "free labour", and (following Antonio Negri) the "social factory": "Simultaneously voluntarily given and unwaged, enjoyed and exploited, free labour on the Net includes the activity of building web sites, modifying software packages, reading and participating in mailing lists and building virtual spaces. For from being an 'unreal', empty space, the Internet is animated by cultural and technical labour through and through, a continuous production of value which is completely immanent in the flows of the network society at large. … In the overdeveloped countries, the end of the factory has spelled out the marginalisation of the old working class, but it has also produced generations of workers who have been repeatedly addressed as active consumers of meaningful commodities. Free labour is the moment where this knowledgeable consumption of culture is translated into excess productive activities that are pleasurably embraced and at the same time often shamelessly exploited. … The new Web was made of the big players, but also of new ways to make the audience work" (Terranova 2004, 74, 78, 95).

Cohen (2008) stresses the need of research on the political economy of web 2.0 and to analyse social networking sites (with special focus on Facebook) in the larger context of commodification and new strategies of capital accumulation under post-Fordist conditions. "In an effort to draw attention to these dynamics, this paper makes two interrelated arguments about the ongoing, extensive commodification in which Facebook is engaged. Extensive commodification refers to the way in which market forces shape and re-shape life, entering spaces previously untouched, or mildly touched, by capitalist social relations (Mosco 1996, 153). Facebook facilitates this process through the valorisation of surveillance. Not only is surveillance the method by which Facebook aggregates user information for third-party use and specifically targets demographics for marketing purposes, but surveillance is the main strategy by which the company retains members and keeps them returning to the site. This leads to the second argument of this paper: it is the unpaid labour of producer-consumers that facilitates this surveillance. Like other Web 2.0 businesses, Facebook is engaged in the commodification of what can be understood as free labour, or what has been called immaterial labour. What distinguishes this particular social network is the way in which surveillance is fundamental to this process. Although Facebook and other Web 2.0 ventures have implemented strategies that break with those of 'old' media, these sites can be situated within more general capitalist processes that follow familiar patterns of asymmetrical power relations between workers and owners, commodification, and the harnessing of audience power" (Cohen 2008, 7-8). For Cohen (2008, 9-10), the conflation of production and consumption and the effort of free labour on web 2.0 must be situated in the context of flexible production under neoliberal and neo-Fordist conditions. Free labour furthermore can be considered as tendency of capital shifting labour costs onto consumers and to bring knowledge, social relationships, and creativity under the logic of

capital accumulation in the digital age. "Web 2.0 as a business strategy can be understood as capital reacting to and attempting to exploit the way in which people seek non-commodified relationships online" (Cohen 2008, 17). Privately owned social networking sites extend work out of the direct production process of factories and offices into society at large in the form of social labour power in order to accumulate capital (Cohen 2008, 17-18).

In the context of social networks, Coté and Pybus (2007, 101) state that corporations circulate digital commodities, which are sold to third parties: "However, its political-economic foundation demonstrates how such user-generated content – immaterial labour 2.0 – is the very dynamic driving new revenue streams. Thus, it is the tastes, preferences, and social narratives found in user entries which comprises the quotidian motherlode of these new revenue streams. It is this user-generated content that spyware and adware monitor to microtarget those same online subjectivities. This is what has excited media conglomerates like News Corp who realize the value of mining these new networked subjectivities to extend existing and produce new markets – indeed, to construct a new paradigm of capitalist market relations. … Part of what enables the management of the immanent networked relations is the juridical forms of the site's 'Privacy Policy' where it is clearly stated that all information recorded on the website can be shared with third parties" (Coté and Pybus 2007, 100).

Petersen (2008) analyses social networking sites in the context of exploitation, free labour, and enclosure. For Petersen (2008), the huge amount of user-generated content, personal information and network structures make it easy for private corporations to deal with this information. "It is when the technological infrastructure and design of these sites is combined with capitalism that the architecture begins to oscillate between exploitation and participation. … In this way the architecture of participation turns into an architecture of exploitation and enclosure, transforming users into commodities that can be sold on the market. … What is seriously needed is a theory of labor that is able to map both exploitation and free labor, along with considering the value using these sites creates for their users" (Petersen 2008).

Scholz (2008) argues: "A fine example of the Web 2.0 Ideology is immaterial free labor, a fairly unpopular and very complex subject. The Web makes people easier to use. By 'surfing' it, people serve their virtual hosts and they are not unhappy about it. Online, service platforms, rather than products are offered and users are encouraged to participate, communities become the brand. The Web makes it possible to 'out–source' many tasks to the users who can create in 'self–service' mode. … They enjoy using these platforms: from entertainment, to staying in touch with friends and family, to chatting, remixing, collaborating, sharing, and gossiping, to getting a job through the mighty power of weak links. It's a tradeoff. Presence does not produce objects but life as such that is put to work and monetary value is created through the affective labor of users who are either not aware of this fact or do not mind it (yet)."

To sum up: many empirical studies focus on individual privacy concerns and individual privacy-related behaviour. In the context of web 2.0, some authors have advanced critiques of this kind of studying privacy and contribute to filling the identified gap with critical arguments. In addition, some authors conducted critical empirical case studies of economic surveillance and targeted advertising and have thereby helped advancing a critique of the political economy of online/web 2.0 surveillance. Also some authors have tried to situate the logic of web 2.0 surveillance in the context of terms such as exploitation and free labour. In the next section, we will present a critical inquiry of empirical research methods.

3.2. Critical Inquiry of Empirical Research Methods

In this sub-section, a critical inquiry of empirical research methods is provided.

Common empirical research studies usually can be divided into two established approaches: positivism and interpretivism (Cecez-Kecmanovic 2007, 1447; Orlikowski and Baroudi 1991; Chen and Hirschheim 2004).

Chen and Hirschheim (2004, 201) say that "the major differences between positivism and interpretivism concerning research are threefold. Ontologically, positivists believe that reality exists objectively and independently from human experiences while interpretivists emphasize the subjective meaning of the reality that is constructed and reconstructed through a human and social interaction process. Epistemologically, positivists are concerned with the hypothetic-deductive testability of theories. Scientific knowledge should allow verification or falsification and seek generalizable results. As such, a causal relationship is usually presented and a tight coupling among explanation, prediction and control is expected (Orlikowski and Baroudi 1991). Interpretivists, by contrast, assume that scientific knowledge should be obtained not through hypothetic-deductive reasoning but through the understanding of human and social interaction by which the subjective meaning of the reality is constructed (Walsham 1995). Methodologically, positivists contend that, to test hypothetic-deductive theory, research should take a value-free position and employ objective measurement to collect research evidence. A quantitative method such as the survey is a typical positivist instrument. Interpretivists, on the other hand, argue that to understand the meaning embedded in human and social interaction, researchers need to engage in the social setting investigated and learn how the interaction takes place from the participants' perspective. Field studies that engage researchers in the real social setting would be more appropriate for generating interpretive knowledge (Orlikowski and Baroudi 1991)".

Chen and Hirschheim (2004, 201f) conclude that positivist research is mostly characterized by: (1) the formulation of hypotheses, models, or causal relationships

among constructs; (2) the use of quantitative methods, although not always necessary, that test theories or hypotheses; and (3) researchers' claims to make objective, value-free interpretations. "Interpretivist studies, in contrast, could be observed through: (1) evidence from a non-deterministic (free will) perspective; (2) researchers' engagement in the specific social and cultural setting investigated; and (3) an analysis based on participants' viewpoints " (Chen and Hirschheim 2004, 201f).

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

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

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

Critical empirical research aims at creating knowledge as a catalyst for change, helping and giving voice to various marginalized groups and stakeholder, playing an active role in transforming practices and social relations, and assisting actors in emancipating themselves (Österle et al. 2005). "This is based on the belief in the power of knowledge – ideally co-produced by researchers and participants in the study – to transform consciousness of actors about their position and ability to act thus engendering action. It is also based on the conviction that it is not only legitimate but that it is indeed an obligation for a researcher to actively engage in the transformation of … practices" (Cecez-Kecmanovic 2007, 1447).

Critical empirical research should try to expose and deconstruct dominant views. Instead of isolating a special phenomenon from its particular societal context, critical empirical research needs to take that into account and investigate economic, political, and cultural conditioning in order to account for the societal context. Adorno (1976, 68) outlines that, in general, social phenomena can be analysed on two different levels: "Some apply to societal totality and its laws of movement, others, in pointed opposition, apply to individual social phenomena which one relates to a concept of society at the cost of obstracization for being speculative. Accordingly, the methods vary". In contrast, Adorno calls for a dialectical approach, which assumes society and the individual as mutually conditioned and interrelated. This relation also has to be considered in conducting empirical research. He points out that "the method is likely both to fetishize its object and, in turn, to degenerate into a fetish" (Adorno 1976, 72). Here Adorno criticizes that empirical research tends to give too much attention to the individual and its power to condition social structures. Thereby social research tends to neglect the societal context, in which the individual is embedded and within which its attitudes, believes, and behaviours are framed.

"By developing a situated understanding of positions and experiences of people affected by the systems, and by linking such understandings with broader conditions, power relations and social structures, critical researchers (co)create knowledge with transformative and emancipatory intent" (Cecez-Kecmanovic 2007, 1446). Instead, the analysis of existing studies on information privacy shows that mainstream empirical research aims at assisting economic actors in achieving their goals and realizing profit interests. Implications derived from the studies tend to be concerned with increasing efficiency and profitability.

Among the analyzed empirical studies, only few can be considered as being critical (for example: Turow et al. 2009, Fuchs 2009; Gilliom 2001). Existing empirical research on online privacy and online surveillance seems to be dominated by the positivist approach, applying positivist, non-critical, and mostly quantitative-only empirical research methods. This finding is consistent with existing studies on the prevalence of different research methodologies in information systems research. For example, Chen and Hirschheim (2004) conducted a study, in which they analyzed 1893

articles (published between 1991 and 2001) in eight major information systems journals in order to assess which kind of research methodologies are most commonly applied. The results clearly showed that with 81% the positivist research methodology dominates the field. A similar study ten years earlier showed similar results: Orlikowski and Baroudi (1991) found that 96,8% of the studies are grounded in the positivist paradigm, only 3,2% in the interpretative paradigm and no empirical research work using a critical paradigm was conducted.

3.2.1. Critical Empirical Methodology

The critical approach is not identified with specific critical methods. Rather, it relies on the appropriation of interpretivist and, to a lesser extent, positivist methods. Therefore it is essential that critical researchers are well aware of the characteristics and limitations of the applied empirical paradigm.

Positivist research methodology is based on empirical testability and replicability of causal relations and theories. It is assumed that empirical phenomena can be accurately and precisely measured. Positivist empirical research aims at obtaining objective facts, which are independent from the method actually used. Cecez-Kecmanovic (2007, 1449) summarizes that "empirical inquiries are required to examine whether hypothesized causal relations are supported/confirmed or rejected by empirical evidence. Negative or disconfirming evidence eliminates, while supporting evidence strengthens a hypothesis of a causal relation. Theories are developed and refined over time through replicated hypothesis testing, elimination of those not supported or confirmed by empirical evidence, generation of new hypothesis and so on, thereby contributing to accumulation of scientific knowledge that leads to progress." In order to achieve valid and generalizable hypotheses, researchers need to apply appropriate scientific methods, create valid samples, and design and administer surveys or design and execute controlled experiments (Cecez-Kecmanovic 2007, 1450).

Interpretive researchers believe that "everyday social practice cannot be disconnected from and studied independently of socially created meaning systems and the language that actors use to describe and make sense of these practices" (Österle et al. 2005, 1449).

Cecez-Kecmanovic (2007) describes how interpretivist empirical researchers work: "they therefore use particular research methods, such as field studies, ethnographies, action research, discourse analysis, etc., to get inside the worlds and meaning systems of those being studied and obtain an in-depth understanding of their subjective beliefs, experiences, feelings and values. Instead of producing research findings as established facts, interpretivist researchers are offering findings as interpretations. Research findings as interpretations are judged based on credibility of the research process, trustworthiness (as a parallel to objectivity) in the research design

and the ways concrete empirical material (observations, interviews, events) are analyzed and interpreted. A new understanding or explanation of the phenomena studied is judged based on the richness of descriptions, internal coherence, depth and insightfulness of interpretations and plausibility of results to a reader. As to the links between a method and a theory, interpretive researchers generally assume that the people's subjective views and beliefs have primacy over the theories that may be 'imposed' on them" (Cecez-Kecmanovic 2007, 1449).

However, interpretive researchers differ in the way they interpret empirical data and derive explanations and theories. For instance, those applying grounded theory (first described by Glaser and Strauss 1967) conduct field studies without a theoretical model or a priori concept and derive theory inductively from data, that is, they ground a theory in the data. An action researcher may start with and apply a theoretical model and through action and learning cycles revise the model and produce empirical evidence to support it (Cecez-Kecmanovic 2007, 1449).

Contemporary critical researchers from different disciplines reinforce the empirical dimension of critical research and the development of critical research methodology (Crotty 1998, Klein 1999, Kincheloe and McLaren 2000). Österle et al. suppose that this development simultaneously emerge in two major directions: "The first direction follows the model of positivist and interpretivist research approaches and assumes that a distinctly critical research approach needs to employ distinctly critical research methods, such as critical ethnography (Thomas 1993), participatory action research (Baskerville 1999), and critical discourse analysis (Fairclough 2010). The second direction of critical methodological developments and debate is more concerned with methodological choices and social and political contexts in which these choices are made" (2005, 1449). Galtung highlights: "To work with any methodology … is a political act … the choice of a methodology is implicitly the choice of an ideology, including the mystifying, monotheistic ideology that there is but one methodology – the universal one. To the extent that we are conscious the choice is for us to make, not to be made for us, and to the extent that we are free for us to enact" (Galtung 1977, 40).

Critical research methodology is explicitly concerned with the choices about linking theories and research methods to any given research context. The task is not so much to develop critical methods, but rather the use of methods for collecting data that allows producing critical knowledge by critically interpreting the data. Cecez-Kecmanovic (2007, 1552) points out that all these requirements and demands can hardly be met by a single method. Therefore some authors recommend a multimethod approach as an essential feature of a critical empirical research approach.

Various empirical methods, as well as quantitative and qualitative approaches, can be combined with the underlying assumptions of critical theory. Adorno (1976, 76) emphasized the combination of quantitative and qualitative research: "The opposition between quantitative and qualitative analysis is not absolute. It is not the last word in the matter. It is well known that whoever quantifies must always first abstract from qualitative differences in the elements, and everything that is societally individual contains the general determinations for which the quantitative generalizations are valid. The proper categories of the latter are always qualitative. A method which does not do justice to this fact and rejects qualitative analysis as incompatible with the essence of the collective realm distorts what it should investigate". Critical research is not afraid of inconsistency, but rather embraces it within a critical dialectical theory. "The eagerness to quantify immediately even the qualitative findings is not fortuitous. Science wishes to rid the world of tension between the general and the particular by means of its consistent system, but the world gains its unity from inconsistency" (Adorno 1976, 77).

However, other authors advise against mixed multi-method approaches. In Davison (2005), Jeff Smith advises against mixing normative arguments about privacy with positivist or interpretivist research. "Such a treatise would not be expected to address research design, sampling procedure, data analysis, and the like, since they mean little in the domain of normative argumentation. In fact, to the extent that data from real world were mentioned in the treatise, they would be solely to further the ethical argumentation" (Davison et al. 2005, 347). He further emphasizes that a critical approach, which uses and combines different elements, will have a harder time being recognized in academic publications. Smith states some concerns: "For example, assume that a privacy researcher wishes to proffer a normative privacy argument – for instance, that individuals' medical information is sacrosanct and that the normative duty of … professionals is to protect it, no matter how much such protection costs. If such a normative argument were well defended under the rules of moral discourse, as established by the discipline of philosophy, the paper might well find a home in a highly ranked journal within that domain. But suppose that, instead, the researcher masks that normative argument by presenting the paper as an interpretive study of hospitals' approaches to medical privacy or as a positivist study of hospital administrators' decision-making regarding privacy issues. Researchers who try such a mixed-category approach sometimes consolidate their normative assertions in the paper's Discussion section, in which case reviewers frequently view them as unfounded since they go far beyond the paper's descriptive findings. Or, even more alarmingly, the researchers simply intersperse their normative assertions covertly throughout the paper so that the Theory, Methods, Analysis, and Results sections read more as value-laden diatribes than as reports of the research Process" (Davison et al. 2005, 349).

There is only little critical empirical research available about privacy and surveillance in general, consumer privacy/surveillance and Internet/web 2.0/SNS pri-

vacy/surveillance. Furthermore, only little qualitative research has been conducted about privacy and surveillance in general. Some qualitative studies have served as a preparation for quantitative studies and produced no independent output (see for example the one of GPD, Chan et al. 2008). Some qualitative research has focused on the analysis of peoples' variability of privacy/surveillance concerns (Ellis, Harper, and Tucker 2010). Another contribution of qualitative research has been to demonstrate dominant surveillance and privacy theories' inappropriateness to express the real attitudes and feelings of concerned people and to assist the victims of surveillance (Gilliom 2001, 41-42; 45; 159, fn3).

Critical privacy and surveillance research should integrate qualitative methods in order to explore peoples' conflicting consciousness, which is based on conflicting capitalist realties. Other than Harper and Slington (2001), who claim that privacy polls and privacy surveys are useless and should not instruct political action because only markets provide proper mechanisms to balance people's different and conflicting interests, critical qualitative empirical research is needed to explore and reveal people's needs that might be suppressed by market mechanisms. For example, assumed that economic privacy (in its strong relationship with private property and individualism) is itself a moment of privacy destruction, qualitative research is a proper way to explore how this conflicting relation of privacy aspects works in peoples' common knowledge and everyday practices. Such qualitative research could contribute to a critical notion of economic privacy, what is missing within the existing literature on offline privacy and surveillance.

3.2.2. A Biased Relationship: Conducting Surveys about Surveillance/Privacy

On a general level, methodological problems of conducting surveys about surveillance and privacy may occur, since surveying itself can be seen as a form of surveillance and privacy intrusion. Gary T. Marx discusses that problem and suggests keeping in mind several questions for judging surveillance such as informed consent, transparency, and reciprocity (Marx 2008).

From a practical point of view, some authors indicate that people of high surveillance/privacy concern are more likely to refuse survey participation. "If the factors that lead certain groups of individuals to be disproportionately excluded from a survey are in some way related to the topic being studied, then the non-response can be a major methodological limitation" (Haggerty and Gazso 2005, 175). This problem might result in "a sample where individuals who we might characterize as being 'pro-surveillance' are over-represented" (Haggerty and Gazso 2005, 175).

Davison et al. (2003) state similar concerns: "The non-response bias problem is an especial challenge. It seems reasonable to assume that distributions of responses from people who are willing to answer questionnaires about privacy topics will be

different from those that would arise if it were possible to obtain responses from those who decline to participate. Moreover, it would seem reasonable to assume that a significant proportion of those who decline do so because they place a high value on privacy. Hence there is likely to be a systematic bias in the data that is gathered, with the level of privacy concern in the population consistently under-stated by the respondent sample" (Davison et al. 2003, 344).

They particularly criticize that "discussion of this problem is almost entirely absent" (Davison et al. 2003, 344). The analysis of existing surveys show that especially studies informed by marketing assumptions tend to neglect that bias. In contrast, critical studies such as Turow et al. (2009) highlight this limitation more prominently. In their survey on attitudes of consumers towards behavioural targeting and tracking, Turow et al. (2009, 10) state: "The particular nature of the topic of this survey makes the findings particularly suspect. One might worry that people who volunteer to participate would feel less concerned about companies using their data online than would a representative sample of adults who use the Internet but would not volunteer for an online survey".

However, among those who did not respond to their survey call, the GPD project team found that very few stated that privacy was a reason (Harling Stalker 2007, 4). So in this case, the assumption of a systematic bias could not be supported empirically. Here further research should be conducted.

Haggerty and Gazso (2005) suggest several practical implications: First, scholars should publicly express structural limitations of research. Second, scholars should list their response rates in detail. Third, scholars should think about weighting their results statistically. Fourth and finally, Haggerty and Gazso call for methodological rigor and political honesty of researchers, who should admit the non-validity of their research if the case arises.

3.3. Methodological Implications of Empirical Research on (Online) Privacy & Surveillance

This sub-section discusses some methodological implications of empirical research on privacy.

In order to operationalize theoretical constructs of critical (economic) privacy and surveillance, which elements can be found in the existing research literature? What research questions, hypothesis, and (sets of) items may be useful for critical empirical research or can be adapted to critical (economic) privacy and surveillance research? What are examples of poorly designed uncritical surveys/empirical research and why are they poorly designed? First, helpful elements in existing studies are outlined; then

secondly, single items according to different dimensions, such as respondents' knowledge, experience, attitude, and behaviour, are discussed.

The qualitative research of the GPD (Ekos 2004, 15) shows that privacy and surveillance is not something that people think about on a day-to-day basis; therefore it is crucial to design research instruments in a way that reflects everyday contexts and experiences of the studied individuals (see for example Nowak and Phelps 1992, Wang and Petrison 1993). Privacy is a complex issue and its meaning depends strongly on the context, within which it occurs. Therefore, providing privacy and surveillance scenarios that are likely to occur or to have occurred in the everyday reality of the respondents seems useful. For this purpose, the social research literature suggests applying the vignettes approach (see for example Finch 1987; Barter and Renold 1999). Finch describes vignettes as "short stories about hypothetical characters in specified circumstances, to whose situation the interviewee is invited to respond" (1987, 105). Barter and Renold list several advantages of this approach: "Vignettes may be used for three main purposes in social research: to allow actions in context to be explored; to clarify people's judgements; and to provide a less personal and therefore less threatening way of exploring sensitive topics. In qualitative research, vignettes enable participants to define the situation in their own terms" (1999). However, there are also objections towards this methodology: "The context that each respondent perceives for the questions is likely to include factors that are extraneous to the designer's intention, that may vary during the course of the data collection, and that may even be unknown to the researcher" (Davison et al. 2003, 343).

Building indexes contributes to a broader reception of empirical research. One can suppose that the popularity of Harris and Westin surveys stems – at least partially – from the expressiveness of their different privacy indexes. For example, Turow et al. used Westin's "Core Privacy Orientation Index" within their own survey (Turow et al. 2009, 21):

	Strongly Agree (%)	Agree (%)	Disagree (%)	Strongly Disagree (%)	Don't Know (%)
Consumers have lost all control over how personal information is collected and used by companies.	20	47	27	4	2
Most businesses handle the personal information they collect about consumers in a proper and confidential way.	5	53	32	6	4
Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.	4	50	34	8	4

Table 19: American's confidence in the way business and the law handle their information (N=1000) (source: Turow et al. 2009, 21)

The advantages of such a questionnaire design are, first, that it takes economic surveillance into consideration (first two items) and, second, that it asks people not only about their capacity to individually control personal data, but but also about the collective dimensions of privacy (referring to law in the third item). Such a research design promises to be fruitful. However, the attitude indexes by Harris and Westin are less elaborated and not fully public, and therefore can be criticized for their interest bias and methodological inconsistency (Gandy 2003, 292; Smith 2006, 4-8). Further research should not borrow from Harris and Westin par for par in a non-reflective manner. Especially Westin's classificatory approach should not be adopted because categories like "pragmatist", "fundamentalist" are highly normative judgments and can be used for manipulating the public towards viewing privacy concerns negatively.

An interesting attempt appears in the conceptual replication of Westin's "General Privacy Concern Index" using items from the GPD project (Margulis, Pope and Lowen 2010; Smith 2006). This methodology allows, at least to some extent, to compare general privacy concerns with Westin's data. According to Margulis, Pope, and Lowen (2010) and Smith (2006), the following items of the GPD questionnaire are feasible for a replication of Westin's index (Zureik et al. 2010, 364-365; 368; 370-371):

- *Item 2: "To what extent do you have a say in what happens to your personal information? Would you say you have…" (answer opportunities: complete say, a lot of say, some say, no say, not sure)*
- *Item 5: "When it comes to the privacy of personal information, what level of trust do you have that the [Insert country of interview] government is striking the right balance between national security and individual rights? Do you have a…" (answer opportunities: very high level of trust, reasonably high level of trust, fairly low level of trust, very low level of trust, not sure)*
- *Item 11: "When it comes to privacy, how worried are you about providing personal information on websites, such as your name, address, date of birth, and gender? Are you…" (answer opportunities: very worried, somewhat worried, not very worried, not worried at all, not sure)*
- *Item 17: "The government of [Insert country of interview] has enacted laws aimed at protecting national security. To what extent do you believe laws aimed at protecting national security are intrusive upon personal privacy? Are they…" (answer opportunities: highly intrusive, somewhat intrusive, not very intrusive, not intrusive at all, not sure)*
- *Item 18: "To what extent do you think it is appropriate for a government agency to share citizen's personal information with third parties, such as other government agencies, foreign governments and the private sector?" (answer opportunities: Yes, it is the government's right under all circumstances, Yes, if the citizen is suspected of*

wrong-doing, Yes, as long as the government has the expressed consent of the citizen, No, under no circumstances should government share information about citizens, not sure; applicable to three options: a) With other government agencies, b) With foreign governments, c) With the private sector)

- *Item 19: "To what extent do you think it is appropriate for a private sector organisation to share or sell its customers' personal information with third parties, such as the national government, foreign governments and other private sector organisations?" (answer opportunities: Yes, it is the organisation's right under all circumstances, Yes, if the citizen is suspected of wrong-doing, Yes, as long as the organization has the expressed consent of the citizen, No, under no circumstances should organizations share information about citizens, not sure; applicable to three options: a) With national government agencies, b) With foreign governments, c) With other private sector organisations)*
- *Item 11 is related to Westin's first question (concern about threats to your personal privacy), item 19 is related to Westin's second question (business organizations seek excessively personal information from consumers), items 5, 17, and 18 are related to Westins third question (government still invading citizen's privacy), and item 2 is related to Westin's fourth question (consumers have lost all control over their information)*

.

For critical research that focuses on consumer privacy, it seems promising to adopt questions from Westin's "Core Privacy Orientation Index" (as Turow et al. 2009 did). For critical research on the perception of governmental surveillance, it seems promising to adopt questions from Westin's "General Privacy Concern Index" or its replication.

However, Westin's claim that attitudes towards more specific privacy related issues are represented in his "General Privacy Concern Index" was not supported by the statistical analysis conducted by Margulis, Pope and Lowen. Instead, they found that "privacy concerns are more than simply a general concern about privacy. Privacy concerns are multi-factorial. They also include how much we feel we can control our private information as well as our beliefs about the appropriateness of governments and private businesses invading our privacy" (2010, 107). Therefore, research has to test if and how general privacy concerns are related to concerns about specific privacy related issues and to non-attitudinal factors, such as experience, behaviour, and knowledge.

The latter fact is stressed by several studies (Gross and Dommeyer 2003; Grenville 2010; Awad and Krishnan 2006, Buchanan et al. 2007; boyd and Hargittai 2010; Christofides, Muise, and Desmarais 2009). They argue theoretically and have found empirically that knowledge, experience, attitudes, and behaviour are interrelated and sometimes contradictory. Further research should consider that it is problematic, for

example, to infer from attitudinal surveys results to the dimension of peoples' behaviour.

Several privacy paradoxes are described within the literature. The most frequently identified privacy paradox is the gap between individuals' intention to disclose private issues and individual's actual disclosure behaviour (Norberg, Horne, and Horne 2007; Barnes 2006). Another paradox is described by Gross and Dommeyer (2003). Their research finds that a high awareness degree of protection strategies from direct marketing activities appears together with a low degree of usage of these strategies. These privacy paradoxes (people are aware of the dangers of sharing personal data, but do it anyway) are specific to capitalist societies. People see at the same time advantages and disadvantages, but have to take the disadvantages into account in order to achieve the advantages. In capitalism these advantages are achieved exactly through the disadvantages. For example, users of social networking sites enjoy free access in order to communicate and stay in contact with friends. In doing so, they consciously accept the use of personal information and thereby exploitation and economic surveillance (Fuchs 2011a). Further research should assess such contradictions and paradoxes within a dialectical analysis of society, which allows situating paradoxes critically.

In the following sections, we classify and discuss several items from existing surveys according to these four dimensions (experience, knowledge, attitudes, behaviour). But, it is crucial to note that measuring one dimension may also require items of other dimensions. For example knowledge about privacy may be affected by respondents' behaviour or experience, which therefore needs to be examined as well.

3.3.1. Analyzing Experiences

To explore people's experience is often similar to explore their knowledge of something. For example, the GPD project asked people for their knowledge about several surveillance technologies, namely the Internet, GPS, RFID on consumer products, CCTV in public spaces, biometrics for facial or other bodily recognition, data mining of personal information (Greenville 2010, 74):

- *"Have you personally, to the best of your knowledge, ever experienced any of the following: Detention at a border checkpoint resulting in a search; Detention by airport officials resulting in not being able to board the airplane; Detention by airport officials resulting in being denied entry into a country; Victim of identity theft (e.g. someone uses your name); Victim of credit card fraud; Your personal information monitored by a government agency; Your personal information monitored by an employer; Your personal information sold by a commercial business?" (answer opportunities: "yes", "no", "not sure")*

However, measuring knowledge and experience is not exactly the same. Experience refers more to a personal involvement. In contrast, knowledge can be acquired indirectly through media reception or having heard relevant stories from family or friends. Therefore knowledge and experience should be assessed in two separate dimensions.

3.3.2. Analyzing Knowledge

When seeking to understand whether American's acceptance or rejection of tailored advertising is related to bad experiences they might have had with information theft, Turow et al. (2009, 19) asked for "bad privacy experiences": Has someone "used or revealed personal information about you without your permission" (it happened to 29%), has someone "made a purchase on your credit card or opened a new credit card in your name without your permission" (that happened to 28%), and if the participant has ever "receive(d) a notice in your postal mail that your personal information has been lost or stolen – for example, in a security breach" (it happened to 31%). Such questions have to be adapted to the respective cultural conditions. For example, in Austria credit card use is way less common and frequent than in the US. In general, one can criticize that Turow et al. defined "bad experience" as harmful actions imposed on the participants by fraudulent individuals. They did not ask for any experienced privacy breaches conducted by economic actors (companies) in a "non-criminal" (but maybe not definitely legal) way.

3.3.3. Analyzing Knowledge

Turow et al. (2009) tried to find out participants' knowledge about privacy by asking them a row of true-or-false questions about privacy laws online and offline. They also provided a "don't know" choice. The first set (privacy online) contained the following statements (for each of them "false" would be the correct answer) (Turow et al. 2009, 21):

- *"If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission.*
- *If a website has a privacy policy, it means that the site cannot give your address and purchase history to the government.*
- *If a website has a privacy policy, it means that the website must delete information it has about you, such as name and address, if your request them to do so.*
- *If a website violates its privacy policy, it means that you have the right to sue the website for violating it.*
- *If a company wants to follow your intent use across multiple sites on the internet, it must first obtain your permission."*

Nowak and Phelps (1993) analysed consumers' knowledge of data sources similarly. They asked respondents for stating if it is true or false that different sources can be used for direct marketing purposes (in the U.S.A.) (Phelbs and Nowak 1993, 30).

Concerning the results of such assesements, one can hypothesize that a slightly more educated sample (like Austrian students) would create somewhat different results than for example found in the Turow et al. study. In addition, especially privacy policies tend to be under attack of "critical" media coverage on privacy in general. This fact could already have resulted in a general higher consciousness of these issues. The questions asked by Turow et al. (2009) are quite critical. It may be interesting to provide participants with an example scenario that illustrates how much can be known about a single user, once all or only multiple sources of data are combined. In contrary, for example, the GPD project (Chan et al. 2008, 8) and Milne and Rohm (2000, 243) explore people's surveillance and privacy knowledge in a different manner. They only ask questions that allow examining peoples' self-assessment of knowledge, but no questions about factual knowledge, as it is possible via true/false questions. Testing factual knowledge of respondents may be a better strategy for achieving reliable results than asking them about their self-assessed state of knowledge because the actual knowledge can be assessed, quantified and knowledge indexes can constructed. Self-assessments of knowledge about privacy and surveillance are unreliable instruments that may create distorted or false results.

Specific behaviour, such as watching news or reading privacy policies of social networking sites, could be a precondition of surveillance and privacy knowledge. Fogel and Nehmad (2009) carried out a quantitative survey with students at a University in New York City (N=205). Participants were asked to complete an anonymous questionnaire with questions such as: "Do you read a website's privacy policy before you register your information?" (5-point scale from 1=never to 5=always) (Fogel and Nehmad 2009, 155). With the help of legal instruments such as privacy policies and terms of use, web 2.0 platforms have the right to store, analyze, and sell personal data of their users to third parties for targeted advertising in order to accumulate profit (Fuchs 2011b). Therefore, we think that such questions are suitable in order to analyze how users are informed what social networking sites are able to do with personal(ly) (identifiable) information. A further strategy is to ask users to check certain privacy settings (for example, Facebook advertising privacy settings) when completing an online survey. Therefore one shows them pictures of how to do it, and to let them report the results of the actual settings. So on the one hand, one can test the general attitudes towards reading privacy policies and terms of use, how much users care about online surveillance, what they think about targeted advertising, etc. On the other hand, one can also test the actual settings they use in applications (such as Facebook) and their factual knowledge about privacy and surveillance (in general and in respect to social media like Facebook).

3.3.4. Analyzing Attitudes

One example of attitude exploring items has already been discussed above (see the section about indexes). Turow et al. (2009) used the questions of Westin's "General

Privacy Concern Index" within their own survey. However, they criticized existing survey-designs that use questions (and refer negatively to Westin's surveys as well) that aim to evaluate consumers' attitudes towards behavioural targeting and tracking. They provided an alternative set of items (Turow et al. 2009, 10-11) and argued: "TRUSTe's questionnaire, fielded two years in a row by TNS, asked about behavioral targeting and tailoring in a way that asked respondents whether they agreed or disagreed with a statement about both activities that also added the promise of anonymity: 'I am comfortable with advertisers using my browsing history to serve me relevant ads, as long as that information cannot be tied to my name or any other personal information'. In response, about 57% said they either strongly agreed (18%) or agreed (39%). The Westin study, conducted by Harris Interactive online, also posed a standalone question about how 'comfortable' people felt with behavioural targeting and tailoring: 'As you may know, websites like Google, Yahoo!, and Microsoft (MSN) are able to provide free search engines or free e-mail accounts because of the income they receive from advertisers trying to reach users on their websites. How comfortable are you when those websites use information about your online activity to tailor advertisements or content to your hobbies or interests?' Westin found that 59% said they were uncomfortable, with younger people (18-24 and 25-29) having lower percentages than older people – though still over 50%. Westin then asked people to assume that 'websites' adopted four stringent privacy and security policies (explaining how the tailoring process would work, offering choices of tailoring, safeguarding information, and promising not to share any user's name or address) and found that now most people apart from those 63+ were 'comfortable' with behavioural targeting and tailoring. Still, the percentages 'not comfortable' despite these stringent standards were substantial – 38% for 18-31 year olds, 44% for 32-43 year olds, 48% for 44-62 year olds and 54% for those 63+" (Turow et al. 2009, 10). So, not only the question was framed in favour of behavioural targeting (by pointing to the benefits of such trade-off i.e. free services), but also the conclusion was drawn that most people are comfortable with behavioural targeting based only on the results of an assumption (i.e. the adoption of four not very common privacy policies). The authors further criticized both these surveys for combining two ideas into one question: "the issue whether sites should serve tailored content and whether the tailoring should be based on a certain kind of tracking" (Turow et al. 2009, 11). Also they identified the problem that none of the surveys say anything about the particular nature of the targeted behaviour, for example both studies did not take into account the possibility that data collected offline might be used to serve tailored ads as well (Turow et al. 2009, 11).

Fogel and Nehmad (2009, 155) also included in their questionnaire statements such as: "I am concerned that the information I submit on the Internet could be misused" (1=strongly disagree to 5=strongly agree) in order to explore Internet users' attitudes. Given the fact that the majority of the most popular web 2.0 platforms such as Facebook and MySpace are privately owned and commercially organized and that

the business model of most commercial web 2.0 platforms is based on personalized advertising (Sandoval 2011), we find statements for a questionnaire about privacy and surveillance on web 2.0 such as "I am concerned that the information I submit on the Internet could be misused" (as used for example in the study by Fogel and Nehmad 2009) as too broad and vague. Rather, we suggest modifying such a statement into: "I am concerned that the information I submit on social networking sites such as Facebook and MySpace could be used for targeted advertising" (1=strongly disagree to 5=strongly agree).

3.3.5. Analyzing Behaviours

Critical research is interested in abolishing asymmetric power structures (Horkheimer 1937/2002; Marcuse 1937; Fuchs 2008) Therefore, "resistance" is a crucial category of critical research on surveillance.

Within the GPD project, resistance action was measured by asking "Have you ever done the following for the purpose of protecting your personal information?" (Zureik et al. 2010, 366), and by using eight corresponding items, which theoretically refer to Marx (2003). The following overview (Grenville 2010, 72) presents these items and classifies them according to Marx's (2003) categories (for each, the answer opportunities "yes", "no", and "not sure" were provided) (Grenville 2010, 72):

- *Refusal: "Refused to give info to a business because you thought it was not needed".*
- *Refusal: "Asked a company not to sell your name and address to another company".*
- *Refusal: "Asked a company to remove you from lists it uses for marketing".*
- *Refusal: "Refused to give info to a gov't agency because you thought it was not needed".*
- *Discover/ counter-surveillance: "Asked a business you were thinking of dealing with about its policies on the collection of consumer info".*
- *Blocking: "Purposefully gave incorrect information about yourself to a marketer".*
- *Blocking: "Purposefully gave incorrect information about yourself to a gov't agency".*
- *Avoidance: "Asked a company to see what personal information, besides billing info, it had about you in its records".*

Grenville created based on his empirical data three groups of typical resistance attitudes and behaviour, namely "informed resisters", "status quo satisfied", and "alienated skeptics". For this purpose, Grenville (2010, 73) mapped out the category of resistance into four further aspects, which refer to the other dimensions of knowledge, experience and attitude. For him, resistance includes knowledge of surveillance, recognition of the experience of being watched, trust (or mistrust) of the watched, and the perception if or not a person has any control over his or her personal information. The three groups are characterized as follows: "Informed resisters, as their name would suggest, are much more likely to have used a whole host of resistance moves. The status quo satisfied, trusting that most uses of personal information are accept-

able to them, have chosen to be less resistant. But there is a large gap between alienated skeptics' discomfort with sharing their personal information and their lack of resistance. It would appear either they do not know how to resist or they believe resistance is futile - or both" (Grenville 2010, 78). Prevalence of these three groups varies extremely among the surveyed countries; no common trend is detectable (Grenville 2010, 80). In terms of the identified aspects of resistance, Grenville concludes that "informed resisters have travelled its length and that their knowledge, experience, and lack of trust have led them to be resistant. Alienated skeptics have travelled the path in a very different way. They are aware that what they don't know can hurt them, but they don't know much more than that. And they feel powerless to change their circumstances. The status quo satisfied know enough to feel secure trusting government and business with their information. Their ease of consent gives them a greater sense of control" (Grenville 2010, 81). Correlation of these groups with demographic data collected by the GPD survey shows that "informed resisters are better educated and wealthier; alienated skeptics are poorer and less well informed; and the status quo satisfied, for the most part, are relatively comfortable middle-class citizens" (Grenville 2010, 80).

This methodological operationalization of resistance by the GPD project is a good example for combining the different dimensions of knowledge, experience, attitude, and behaviour. However, such an assessment of surveillance resistance is problematic as it is individualistic and does not identify options of collective resistance (like demonstrations, consumer protection agencies, online watch platforms, etc). In order to assess collective forms of resistance against surveillance, one could ask for example:

- *"Have you heard about the existence of any concrete privacy or anti-surveillance movements? Have you been actively involved in such activities?"*

Andrade, Kaltcheva and Weitz (2002) examined in an exploratory study how companies can influence consumers' concerns about self-disclosure of personal data on the Internet. They assume that consumers' willingness to disclose personal information is based on their assessment of the costs and benefits. One of three identified approaches for influencing consumers' willingness to disclose personal data was offering a reward (e.g. coupons, gifts). They operationalized this assumption by showing participants the following statement: "Simply register with us and tell us a little more about yourself. You will receive a $10 check. Don't miss this opportunity". Framing this question with this kind of statement sets a very clear context for participants, as well as appears highly true-to-life (since that is exactly how consumer loyalty programmes do it). Of course, further research should also try to operationalize more subtle forms of offering customers and user benefits. In context of web 2.0 applications, offered rewards may be vouchers for online shopping, free games, birthday reminders, or applications, which allow to post users' whereabouts. On social networking sites users may perceive social advantages as major benefits. From a critical point

of view, it is crucial to stress that the corresponding applications are meant as nothing else than rewards for providing personal data, if a social networking platform is of commercial character.

Debatin et al. (2009) realized an online quantitative (N=119) research with undergraduate students at a US academic institution. In order to study users' practices with regard to privacy, the participants were asked "how they protected their profile (survey options mirrored actual Facebook options: 'I'm not sure,' 'All of my networks and all of my friends can see it,' 'some of my networks and some of my friends can see it,' 'only my friends can see it,' and 'I have different settings for different parts of my profile.')" (Debatin et al. 2009, 91). Christofides, Muise, and Desmarais (2009) ask questions to read into users' behaviour, for example: "How likely are you to say no to a Facebook friend's request in order to control who has access to your information" (7-item scale)? However, web 2.0 activities such as creating profiles and sharing ideas on Facebook, announcing personal messages on Twitter, uploading or watching videos on YouTube, and writing personal entries on Blogger, enable the collection, analyzes, and sale of personal data by commercial web platforms. If I want to share information on commercial social networking sites, I do not have control over my information regardless of my profile settings, because web platforms are allowed legally to use my information in order to generate profit (Andrejevic 2010, 89). Therefore, it is more appropriate asking users if they use opt-out solutions of targeted advertising on social networking sites (if available).

4. Conclusion

In order to summarize the discussion, the following guidelines for critical empirical studies of (online) privacy and surveillance can be formulated:

- What is missing within current research on privacy and surveillance, is a critique of the political economy of privacy and surveillance that takes into account the larger societal context of class, ideology, and exploitation.
- Privacy research should not be solely based on control theories of privacy. Collective notions of privacy and surveillance threats should be explored critically as well.
- Critical empirical research is linked to critical theory, it is not stand-alone research and does not solely focus on the actor as fetishized subject, but rather takes the societal context into account. Critical social research acknowledges contradictory findings and links them to a dialectical analysis of society. Critical empirical research aims at creating knowledge as a catalyst for change in order to abolish domination.
- A multi-method approach, combining quantitative and qualitative social research, is an essential feature of a critical empirical research approach. Combining different methods allows assessing complex and sometimes contradictory data.

- Privacy and surveillance research should be aware of a potential non-response bias.
- Building indexes in combination with classifying people into groups of different qualities is a good way of presenting survey results. However indexes about general concerns are not automatically a predictor of concerns towards related sub-issues. The representative status of such indexes should be tested case by case.
- Scenarios are frequently used in privacy and surveillance research. This methodology has the advantage of helping the respondents to frame abstract and complex topics such as privacy and surveillance in concrete situations that relate to their own experiences.
- It is crucial to have in mind that survey questions can refer to different dimensions, such as knowledge, experience, attitude, and behaviour. One cannot easily infer results from one dimension to another. In addition most categories should include items referring to more than one dimension.
- Knowledge should be explored with "true or false"-questions and not by self-assessment. Otherwise, not really knowledge, rather individual assessment of knowledge would be examined. It is likely that people find their knowledge about surveillance more detailed than it actually is..
- The design of attitudinal items is a sensitive issue because they tend to be leading questions.
- Analyzing resistance to surveillance should be based on collective notions of resistance.
- Benefits that lead people to give up their privacy and to accept surveillance, need to be understood in a broad sense. A benefit can be a financial or economic offer as well as a social advantage. In capitalism, people often can achieve advantages exactly through accepting disadvantages. A dialectical analysis of society is needed for empirical research.

- Many authors focus on individual privacy concerns and individual privacy-related behaviour. Given the fact that the majority of the most popular web 2.0 platforms such as Facebook and MySpace are privately owned and commercially organized and that the business model of most commercial web 2.0 platforms is based on personalized advertising, we find it more appropriate to study web 2.0 in the context of economic surveillance and targeted advertising. This includes, for example:
  - analysing users' knowledge of privacy policies and terms of use,
  - asking users in a survey to check and give information about the privacy settings of their profiles on social media platforms, asking users if they have used opt-out solutions of targeted advertising on social networking sites (if available) and if they know about the availability of these settings (if available).

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*, edited by Phillipe Golle and George Danezis, 36-58. Cambridge: Robinson College.

Adorno, Theodor W. "Sociology and Empirical Research." in *The Positivist Dispute in German Sociology*, translated by Glyn Adey and David Frisby (London: Heinemann, 1976), pp. 68-86.

Alby, Tom. 2007. *Web 2.0: Konzepte, Anwendungen, Technologien*. München: Hanser.

Andrade, Eduardo, Velitchka Kaltcheva, and Barton Weitz. 2002. "Self-Disclosure on the Web: The Impact of Privacy Policy, Reward, and Company Reputation." In *Proceedings of 32nd Annual Conference of the Association-for-Consumer-Research (Acr)*, edited by Susan Broniarczyk and Nakamoto Kent, 350-353. Austin: Association for Consumer Research.

Andrejevic, Mark. 2010. "Social Network Exploitation." In *A Networked Self: Identity, Community, and Culture on Social Network Sites*, edited by Zizi Papacharissi, 82-101. New York: Routledge.

Awad, Naveen Farag, and Mayuram Krishnan. 2006. "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization." *MIS Quarterly* 30 (1): 13-28.

Barter, Christine, and Emma Renold. 1999. "The use of vignettes in qualitative research." *Social Research Update* 25. http://sru.soc.surrey.ac.uk/SRU25.html.

Beer, David and Roger Burrows. 2007. "Sociology and, of and in Web 2.0: Some Initial Considerations." *Sociological Research Online* 12 (5).

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

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

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

boyd, danah, and Eszter Hargittai. 2010. "Facebook Privacy Settings: Who Cares?" *First Monday* 15 (8). Accessed December 16, 2010. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589

Buchanan, Tom, Carina Paine, Adam Joinson, and Ulf-Dietrich Reips. 2007. "Development of Measures of Online Privacy Concern and Protection for Use on the Inter-

net." Journal of the American Society for Information Science and Technology 58 (2): 157-165.

Burg, Thomas, ed. 2003. *BlogTalks*. Norderstedt: Books on Demand.

Burg, Thomas, ed. 2004. *BlogTalks 2.0*. Norderstedt: Books on Demand.

Campbell, Alexandra J. 1997. "Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy." *Journal of Direct Marketing* 11 (3): 44-57.

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

Chan, Yolande E., L. Lynda Harling Stalker, and David Lyon. *The Globalization of Personal Data Project: An international survey on privacy and surveillance: Summary of findings*. Kingston: Queen's University.

Chen, Wenshin, and Rudy Hirschheim. 2004. "A paradigmatic and methodological examination of information systems research from 1991 to 2001". Information Systems Journal 14 (3): 197-235.

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

Cohen, Nicole. 2008. "The Valorization of Surveillance: Towards a Political Economy of Facebook." *Democratic Communiqué* 22 (1): 5-22.

Coté, Mark, and Jennifer Pybus. 2007. "Learning to Immaterial Labour 2.0: Myspace and Social Networks." *ephemera* 7 (1): 88-106.

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

Culnan, Mary. 1993. "How did they get my name? An exploratory investigation of consumer attitudes towards secondary information use." MIS Quarterly 17 (3): 341-363.

Davison, Robert M, Roger Clarke, Xamax Consultancy, and H. Jeff Smith. 2003. "Information Privacy in a Globally Networked Society." Communications of the Association for Information Systems 12(1): 341-365.

Debatin, Bernhard, Jennette Lovejoy, Ann-Kathrin Horn, and Brittany Hughes. 2009. "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences." *Journal of Computer-Mediated Communication* 15 (1): 83-108.

Dommeyer, Curt J., and Barbara L. Gross. 2003. "What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies." *Journal of Interactive Marketing* 17 (2): 34-51.

Dwyer, Catherine, Starr Hiltz, and Katia Passerini. 2007. "Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace." In *Pro-*

ceedings of the 13th Americas Conference on Information Systems. Keystone: Association for Information Systems.

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

Ekos. 2004. Globalization of Personal Data Project: International survey: Findings from the pre-survey focus groups. http://www.sscqueens.org/sites/default/files/Canada_FG_Findings_Ekos_May_2004.pdf.

Ellis, Darren, Dan Harper, and Ian Tucker. 2010. The organisation of life: everyday experiences of surveillance and dataveillance technologies: Paper presented at the political economy of surveillance workshop, Milton Keynes.

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): 1143-1168.

Etzioni, Amitai. 1999. *The limits of privacy*. New York, NY: Basic Books.

Fairclough, Norman. 2010. Critical Discourse Analysis: The Critical Study of Language. 2nd ed. Longman.

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

Finch, Janet. 1987. "The vignette technique in survey research." *Sociology* 21 (1): 105-114.

Fogel, Joshua, and Elham Nehmad. 2009. "Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns." *Computers in Human Behavior* 25 (1): 153-160.

Fried, Charles. 1968. "Privacy." *The Yale Law Journal* 77 (5): 1461-1543.

Fuchs, Christian. 2008. "Towards a critical theory of information." In *Qué es Información? (What is Information?) Proceedings of the First Itnernational meeting of Experts in Infromation Theories. An Interdisciplinary Approach (Primer Encuentro Internactional de Expertos Teorías de la Información. Un enfoque interdisciplinar)*, ed. José Diaz Nafria and Salto Alemany. León: Universidad de León.

———. 2009. *Social Networking Sites and the Surveillance Society: A Critical Case Study of the Usage of studiVZ, Facebook, and MySpace by Students in Salzburg in the Context of Electronic Surveillance*. Salzburg: Research Group Unified Theory of Information.

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

———. 2010b. "studiVZ: Social Networking Sites in the Surveillance Society." *Ethics and Information Technology* 12 (2): 171-185.

———. 2011a. "An Alternative View of Privacy on Facebook." Information 2 (1): 140-165. [special issue on "Trust and privacy in our networked world", edited by Dieter M. Arnold and Herman T. Tavani].

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

———. 2011c. "The political economy of privacy." *SNS3 Research Paper* 8.

Galtung, Johan. 1977. Methodology and ideology. Essays in methodology. International Peace Research Institute, Oslo.

Gandy, Oscar H. 2003. "Public opinion surveys and the formation of privacy policy." *Journal of Social Issues* 59 (2): 283-299.

Geuss, Raymond. 2001. *Public goods, private goods*. Princeton, NJ: Princeton University Press.

Gilliom, John. 2001. *Overseers of the poor: surveillance, resistance, and the limits of privacy*. Chicago, IL: University of Chicago Press.

Grenville, Andrew. 2010. "Shunning surveillance or welcoming the watcher? Exploring how people traverse the path of resistance." In *Surveillance, privacy, and the globalization of personal data: International comparisons*, ed. Elia Zureik, L. Lynda Harling Stalker, Emily Smith, David Lyon, and Yolande E. Chan, 70-83. Montreal: McGill-Queen's University Press.

Habermas, Jürgen. 1991. *The structural transformation of the public sphere: an inquiry into a category of bourgeois society*. Cambridge, MA: MIT Press.

Haggerty, Kevin D. 2006. "Tear down the walls: On demolishing the panopticon." In *Theorizing surveillance: the panopticon and beyond*, ed. David Lyon, 23-45. London: Willan.

Haggerty, Kevin D., and Amber Gazso. 2005. "The public politics of opinion research on surveillance and privacy." *Surveillance & Society* 3 (2/3): 173-180.

Haggerty, Kevin D., and Richard V. Ericson. "The surveillant assemblage." *British Journal of Sociology* 51 (4): 605-622.

Harling Stalker, L. Lynda. Every word counts: Writing the international survey on privacy and surveillance. Background paper of the Globalization of Personal Data Project. http://www.sscqueens.org/sites/default/files/1_Lynda_Harling_Stalker_Web_Paper.pdf.

Harper, Jim and Solveig Singleton. 2001. With a grain of salt: What consumer privacy surveys don't tell us. Retrieved from: http://cei.org/PDFs/with_a_grain_of_salt.pdf.

Harris Interactive. 2001a. Consumer privacy attitudes and behaviors survey, conducted for the Privacy Leadership Initiative: Summary of findings. Harris Interactive, Inc.

———. 2001b. Privacy on & off the Internet: What consumers want. Technical Report, November 2001. Harris Interactive, Inc.

Harris, Louis, and Alan F. Westin. 1990. Consumers in the information age: Findings from the survey. Equifax.

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

———. 1994. Harris-Equifax Consumer Privacy Survey 1994: Executive summary: Major findings of the survey. Equifax. http://www.frogfire.com/frogfire_archive/equifax/consumers/privacy_survey/privacy_survey_1994.html.

———. 1995. Harris-Equifax Consumer Privacy Survey 1995: Executive summary: Major findings of the survey. Equifax. http://www.frogfire.com/frogfire_archive/equifax/consumers/privacy_survey/privacy_survey_1995.html.

———. 1996. Harris-Equifax Consumer Privacy Survey 1996: Executive summary: Major findings of the survey. Equifax. http://www.frogfire.com/frogfire_archive/equifax/consumers/privacy_survey/privacy_survey_1996.html.

Hinduja, Sameer, and Justin Patchin. 2008. "Personal Information of Adolescents on the Internet: A Quantitative Content Analysis of MySpace." *Journal of Adolescence* 31 (1): 125-146.

Horkheimer, Max. 1937. "Traditional and critical theory." In *Critical theory*, 188-252. New York: Continuum.

———. 1972. *Critical theory: selected essays*. Herder and Herder.

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

Kamaraguru, Ponnurangam, and Lorrie Faith Cranor. 2005. Privacy indexes: A survey of Westin's studies: Research report. http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf.

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.

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.

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.

MacKinnon, Catharine. 1989. *Towards a feminist theory of the state*. Cambridge, MA: Harvard University Press.

Marcuse, Herbert. 1937. „Philosophie und kritische Theorie.“ In *Schriften*, 3:227-249. Frankfurt am Main: Suhrkamp.

———. 1968. Negations; essays in critical theory. Beacon Press.

Margulis, Stephen T., Jennifer A. Pope, and Aaron Lowen. 2010. “The Harris-Westin index of general concern about privacy: An exploratory conceptual replication.” In *Surveillance, privacy, and the globalization of personal data: International comparisons*, ed. Elia Zureik, L. Lynda Harling Stalker, Emily Smith, David Lyon, and Yolande E. Chan, 91-109. Montreal: McGill-Queen’s University Press.

Marx, Gary T. 2003. A tack in the shoe: Neutralizing and resisting the new surveillance. Journal of Social Issues 59 (2): 369-390.

Marx, Gary T. 2008. Surveys and Surveillance. In *Envisioning the survey interview of the future*, ed. Frederick G. Conrad and Michael F. Schrober, 254-266. Hoboken: John Wiley & Sons.

Marx, Karl. 1843. On the Jewish question. In *Writings of the young Marx on philosophy and society*, 216-248. Indianapolis: Hackett.

———. 1844. Economic and philosophic manuscripts of 1844. In *Economic and philosophic manuscripts of 1844 and the Communist manifesto*, 13-168. Amherst: Prometheus.

———. 1867. *Capital: A critique of political economy: Volume One*. Middlesex: Penguin.

Mill, John Stuart. 1965. *Principles of political economy*. London: University of Toronto Press.

Milne, George R., and Andrew J. Rohm. 2000. “Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives.” *Journal of Public Policy & Marketing* 19 (2): 238-249.

Milne, George, Andrew Rohm, and Shalini Bahl. 2004. "Consumers' Protection of Online Privacy and Identity." Journal of Consumer Affairs 38 (2): 217-232.

Miyazaki, Anthony, and Ana Fernandez. 2001. "Consumer Perceptions of Privacy and Security Risks for Online Shopping." Journal of Consumer Affairs 35 (1): 27.

Nowak, Glen J., and Joseph E. Phelps. 1992. “Understanding privacy concerns: An assessment of consumers' information-related knowledge and beliefs.” *Journal of Direct Marketing* 6 (4): 28-39.

Phelps, Joseph, Glen Nowak, and Elizabeth Ferrell. 2000. “Privacy Concerns and Consumer Willingness to Provide Personal Information.” *Journal of Public Policy & Marketing* 19 (1): 27-41.

O’Reilly, Tim 2005. “What Is Web 2.0?” Retrieved from: http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html?page=1

Orlikowski, Wanda J., and Jack J. Baroudi. 1991. “Studying Information Technology in Organizations: Research Approaches and Assumptions.” Information Systems Research 2(1): 1-28.

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

Petersen, Søren Mørk. 2008. "Loser Generated Content: From Participation to Exploitation." *First Monday* 13 (3). Accessed January 24, 2011. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2141/1948

Phelps, Joseph, Glen Nowak, and Elizabeth Ferrell. 2000. Privacy concerns and consumer willingness to provide personal information. Journal of Public Policy & Marketing 19: 27-41.

Posner, Richard A. 1978. An economic theory of privacy. In *Philosophical dimensions of privacy: an anthology*, ed. Ferdinand Schoeman, 333-345. Camebridge: Cambridge University Press.

Rachels, James. 1975. “Why privacy is important.” *Philosophy and Public Affairs* 4 (4): 323-333.

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

Saveri, Andrea, Howard Rheingold, and Kathi Vian. 2005. Technologies of Cooperation. Palo Altho: Institute for the Future.

Scholz, Trebor. 2008. "Market Ideology and the Myths of Web 2.0." *First Monday* 13 (3). Accessed February 7, 2011. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2138/1945

Sheehan, Kim. 2002. "Toward a Typology of Internet Users and Online Privacy Concerns." *The Information Society* 18 (1): 21-32.

Shirky, Clay. 2008. *Here Comes Everybody: The Power of Organizing without Organizations.* London: Penguin.

Smith, Emily. 2006. Comparing the Globalization of Personal Data survey on privacy and surveillance to Alan Westin's survey results and the privacy dynamic. http://www.sscqueens.org/sites/default/files/5_Smith_WestinComparison_May06.pdf.

Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke. 1996. "Information privacy: Measuring individuals' concerns about organizational practices." *MIS Quarterly* 20 (2): 167-196.

Terranova, Tiziana. 2004. *Network Culture: Politics for the Information Age.* London: Pluto Press.

Turow, Joseph, and Michael Hennessy. 2007. "Internet Privacy and Institutional Trust: Insights from a National Survey." *New Media Society* 9 (2): 300-318.

Turow, Joseph, Lauren Feldman, and Kimberly Meltzer. 2005. "Open to Exploitation: America's Shoppers Online and Offline." Annenberg School for Communication Departmental Papers.

Turow, Joseph, Michael Hennessy, and Amy Bleakley. 2008. "Consumers' Understanding of Privacy Rules in the Marketplace." *Journal of Consumer Affairs* 42 (3): 411-424.

Turow, J., J. King, C.J. Hoofnagle, A. Bleakley, and M. Hennessy. 2009. Contrary to what marketers say, Americans reject tailored advertising and three activities that enable it. University of Pennsylvania and Berkeley Center for Law & Technology. Available at SSRN: http://ssrn.com/abstract=1478214

Walsham, G. 1995. "Interpretive case studies in IS research: nature and method." *European Journal of Information Systems* 4 (2): 74-81.

Wang, Huaiqing, Matthew Lee, and Chen Wang. 1998. "Consumer Privacy Concerns About Internet Marketing." Communications of the ACM 41 (3): 63-70.

Wang, Paul, and Lisa A. Petrison. 1993. "Direct marketing activities and personal privacy: a consumer survey." *Journal of Direct Marketing* 7 (1): 7-19.

Zureik, Elia, L. Lynda Harling Stalker, Emily Smith, David Lyon, and Yolande E. Chan, eds. 2010. *Surveillance, privacy, and the globalization of personal data: International comparisons*. Montreal: McGill-Queen's University Press.

Zureik, Elia, and L. Lynda Harling Stalker. 2006. Background paper for the Globalization of Personal Data Project international survey on privacy and surveillance. http://www.sscqueens.org/sites/default/files/Background%20Paper.pdf.

Zureik, Elia. 2004a. Globalization of Personal Data Project: International survey concept paper. Discussed at the 3 March, 2004 SSHRC-funded workshop at Queen's University. http://www.sscqueens.org/sites/default/files/concept_paper.pdf.

———. 2004b. Overview of public opinion research regarding privacy: Appendix A to Globalization of Personal Data Project: International survey concept paper. Dis-

cussed at the 3 March, 2004 SSHRC-funded workshop at Queen's University. http://www.sscqueens.org/sites/default/files/Overview_Appendix_A.pdf.

———. 2010. "Cross-cultural study of surveillance and privacy: Theoretical and empirical observations." In *Surveillance, privacy, and the globalization of personal data: International comparisons*, ed. Elia Zureik, L. Lynda Harling Stalker, Emily Smith, David Lyon, and Yolande E. Chan, 348-360. Montreal: McGill-Queen's University Press.