Online privacy concerns and legal assurance: A user perspective

Article · February 2013

DOI: 10.14763/2013.1.107

Hanna Krasnova
Universität Potsdam

Online Privacy Concerns and Legal Assurance:

A User Perspective

Dr. Hanna Krasnova
Humboldt-Universität zu Berlin
Insitute of Information Systems
krasnovh@wiwi.hu-berlin.de

Paula Kift
Alexander von Humboldt Institute
for Internet and Society (HIIG)
pkift@alumni.princeton.edu

Keywords
Internet, Social Networking Sites, Facebook, Privacy, Privacy Calculus, Legal Remedies.

INTRODUCTION

Since the emergence of the Internet, privacy concerns have been in the spotlight of public attention. The reasons for this include unprecedented possibilities to collect, store, aggregate and analyze user data. Indeed, as users navigate through a myriad of web-sites, their browsing patterns, preferences and demographics can be captured and used for various purposes. These can range from marketing to criminal uses such as identity theft or stalking. In addition, the proliferation of Social Media platforms, such as Facebook, has resulted in a surge of user sharing activity with users revealing an astounding depth and breadth of details about themselves or others in non-anonymous settings. For example, Facebook users are reported to share a whopping *30 billion pieces of content* - web links, news stories, photo albums, notes, just to name a few - *each month*, with Facebook currently representing the largest database of social information in the world (Pring 2012). While engagement in online communication and broadcasting helps users to keep in touch, maintain relationships, and gain emotional support (Koroleva et al. 2011), critics increasingly voice their concerns over privacy threats implied by information sharing of this magnitude. Considering the severity of these concerns, policy-makers around the world are searching for viable solutions to address these problems.

However, finding effective legal means to protect user privacy online has proved to be a formidable challenge. Privacy scholars offer a number of explanations for the complexity of the problem. First, policy-makers and users themselves struggle to find an exact definition and adequate level of privacy protection,as privacy is often used as an "umbrella term" for a variety of meanings and situations (Solove 2002; 2006). As a result, regulation in one area would not necessarily mean protection in another. This lack of a uniform understanding becomes evident when privacy concerns are captured or measured in surveys, with most privacy measurement instruments being too general to reflect the true essence of privacy-related anxiety (Harper and Singleton 2001). Additionally, privacy scholars and policy-makers have been consistently bewildered by the apparent dichotomy between asserted privacy concerns and actual user behavior, with numerous studies revealing a yawning gap between how users claim to feel about privacy and how they act in real-life settings (e.g. Spiekermann et al. 2001; Aquisti and Gross 2006). These inconsistencies lead to scepticism as to the necessity for policy-makers to safeguard user privacy, with some stakeholders arguing that privacy interest should rather be seen as an area of individual responsibility and self-determination.

Contributing to the public and scholarly debate on how privacy can best be addressed and protected, this paper discusses state-of-the-art research on user attitudes and behaviour with regard to online privacy. Particular attention is paid to (1) users' privacy concerns when using the Internet in general and Facebook in particular, (2) attitudes towards legal assurances and (3) willingness to take the initiative on privacy protection. We have chosen Facebook to showcase the particularity of privacy issues in Social Media, due to its sheer size, cross-cultural adoption and documented user engagement (Alexa 2012). To support our line of argumentation we rely on the results of a study conducted with 553 students and staff at a major German university. Conducted between August 9th and 10th 2012, the results of our online survey represent the most recent insights on user attitudes towards privacy. In order to facilitate the reading, this paper is structured as follows: We begin by introducing the reader to the design and sampling of our survey. We subsequently discuss a variety of topics related to online privacy from a user perspective. We then draw on our findings to provide more substance to the discussion, to strengthen our arguments and to provide an overview of the most recent developments in user attitudes towards privacy in a social media setting.

EMPIRICAL STUDY: SURVEY DESIGN AND SAMPLING

To gain a better understanding of users' privacy concerns, their actual online behaviour and the perceived effectiveness of legal assurances, an online survey has been conducted. All questions were initially formulated in English and then carefully translated into German, since respondents were primarily of German descent The survey consisted of *three* parts. In the first part, questions relating to *privacy concerns* and *legal assurances* in a general *Internet context* were posed. This part included a "filter" question on the use of Facebook. Respondents, who answered *affirmatively* to this question, were forwarded to the second part of the survey, where *Facebook-related* questions were asked. In the final third part respondents' *demographic information* was collected. Due to space limitations, we refrain from describing the survey questions in a separate part of this paper, but rather present them in the course of our analysis below.

The mean processing time of the survey amounted to 10 minutes and 29 seconds (median 8 minutes and 18 seconds), providing evidence that that the survey was rather short. As a result, no fatigue-related effects should be expected. The survey was advertised using the mailing list of a major university in Berlin, Germany, and was presented as a study of "*opinions of Internet users*" to avoid fixing respondents on privacy up front. A raffle of 20 €5 and 10 €15 Amazon.de gift cards was offered as an incentive to participate in the study. In total, *553* respondents took part in the Internet-related part of the survey. *403* respondents stated to use Facebook and answered the second part of the survey as well.

Table 1: Basic Demographic Characteristics

Category	Overall Sample n=553	Facebook Sample n=403	Category	Overall Sample n=553	Facebook Sample N=403
Gender	**Share, %**	**Share, %**	**Educational Background**	**Share, %**	**Share, %**
Male	41,6	37,8	Languages / Culture Studies	21,8	22,0
Female	58,4	62,2	Social Studies	11,5	10,9
Highest Degree Reached	**Share, %**	**Share, %**	Business / Economics	7,3	8,3
Less than high school	0,2	0,3	History	5,7	5,6
High school	52,8	52,9	Psychology	5,0	5,8
Vocational training	4,0	3,0	Law	4,2	4,8
Univ. of Applied Sciences	0,9	0,8	Computer Science	3,3	2,8
Bachelor / Diploma	31,9	31,3	Math	2,9	2,3
Univ. Master Degree	8,5	9,8	Other	38,3	37,6
Univ. Doctoral Degree	0,4	0,5			
Employment Status	**Share**	**Share, %**	**Age**	**Statistics**	**Statistics**
Student	89,3	89,9	Mean	25,08	24,77
Employed	5,4	4,3	Median	24	24,00
Other	5,4	5,8	SD	4,196	3,629
Country	**Share**	**Share, %**	Min	17	17
Germany	95,0	94,7	Max	54	40
Other	5,0	5,3			

Table 1 and 2 reveal respondents' demographic characteristics and Facebook usage statistics, respectively. Due to the chosen sampling procedure, the majority of respondents were *students* and came from *Germany*. 96,6% of Facebook users in our sample were between 18-34 years old. Considering that users within this age category constitute the largest Facebook demographic - 55% of all Facebook users are between 18 and 34 (CVP Marketing Group 2011; Hampton et al. 2011) - our sample draws on the most representative part of the Facebook population. Moreover, Kruglanski (1975) argues that student samples are acceptable as long as the research question revolves around general psychological constructs. Nonetheless, a reader should be cautious in extrapolating the results of our survey to other population groups.

Table 2: Usage Patterns of 'Facebook Sample'

Time on Facebook	Share, %	Privacy Settings	Share, %
Less than 5 minutes	10,5	„Friends Only“	61,2
5-10 minutes	18,0	„Customized“	30,5
11-20 minutes	17,3	„Open - Public“ Profile	1,3
21-30 minutes	13,8	Other	7,1
31-40 minutes	8,3	**Number of Friends**	**Statistics**
41-50 minutes	4,0	Mean	191,6
51-60 minutes	10,5	Median	160
between 1 and 1,5 hour	7,5	SD	137,525
between 1,5 and 2 hour	5,8	Min	1
More than 2 hours	4,3	Max	723

In terms of Facebook use, 59,6% of users in our sample spend up to 30 minutes per day on Facebook. This is in line with the global monthly average of 24,3 minutes reported by Alexa (2012). There were no significant differences in the mean number of Facebook friends between male and female users, with the median reaching 191,6 friends. 91,7% of the respondents in our sample made use of friends-only or customized privacy settings in order to limit the access to their user profiles. Only a marginal share of 1,3% made their profile accessible to everyone. Apparently, there is an increasing awareness of privacy concerns among Social Media users with restricted profiles becoming the norm.

WHAT IS PRIVACY?

Despite numerous attempts to find effective legal measures to protect user online privacy, this task has proven to be a formidable challenge. The lack of a holistic definition is one of the explanations for this phenomenon. Solove (2002) discusses six major definitions suggested in the past: 1*) the right to be let alone*; 2) *limited access to the self*; 3) *secrecy*; 4) *control over personal information*; 5) *personhood* and 6) *intimacy*. He argues that while each of these definitions has to some extent been reflected in policy-making, these definitions are either to narrow or too broad to offer the solid foundation for a legal framework. According to Solove (2002; 2006) any attempt to derive a comprehensive definition of privacy is doomed to fail as the term "privacy" is used to describe a multitude of situations and contexts: "*Privacy is a concept in disarray. Nobody can articulate what it means. As one commentator has observed, privacy suffers from "an embarrassment of meaning"* (Solove 2006, p. 477). Against this background, it becomes apparent why privacy protection has proved so difficult to achieve. After all, it is hard to protect something meaningfully, which has not, even yet, been defined (Solove 2002; 2006). Being a legal scholar, Solove (2006) promotes a bottom-up definition of privacy, in which privacy is seen as a complex web of similar, but yet distinguishable phenomena. Specifically, he differentiates between *four types of harmful activities*: *Information Collection* (including Surveillance and Interrogation); *Information Processing* (including Aggregation, Identification, Insecurity, Secondary Use and Exclusion); *Information Dissemination* (including Breach of Confidentiality, Disclosure, Exposure, Increased Accessibility, Blackmail, Appropriation and Distortion); and *Invasions* (Intrusion; Decision Interference). As technologies progress, other types of harmful activities can emerge. For example, within the context of Social Networking Sites (SNSs), Hogben (2007) differentiates between the following *four types of principal threats*: *Privacy Related Threats* (including Digital Dossier Aggregation; Secondary Data Collection; Face Recognition; Content-based Image Retrieval; Linkability from Image Metadata; Tagging and Cross-profile Images; and Difficulty of Complete Account Deletion); *SNS Variants of Traditional Network And Information Security Threats* (including SN Spam; Cross Site Scripting, Viruses and Worms and SNS Aggregators); *Identity Related Threats* (including Spear Phishing using SNSs and SN-specific Phishing, Infiltration of Networks Leading to Information Leakage, and Profile-squatting and Reputation Slander through ID Theft); and *Social Threats* (including Stalking, Bullying and Corporate Espionage).

DO USERS CARE ABOUT PRIVACY?

In response to rising threats, *privacy concerns* are likely to emerge. However, discussing the observed dichotomy between *stated* privacy concerns and *actual* behaviour, numerous scholars question whether people are truly concerned about their privacy, suggesting that privacy concerns may not be as salient as often assumed (e.g. Spiekermann et al. 2001). Indeed, privacy has never been a key subject of US election campaigns (Harper and Singleton 2001). To verify this proposition, Acquisti and Gross (2006, p. 6) have surveyed 294 US respondents - students, staff and faculty of Carnegie Mellon University - asking them to rate the importance of several issues for their own life. They find that "privacy policy" is viewed as a highly important issue, outweighing the importance of such topics as "threat of terrorism" and "same sex marriage". It was, however, less important than "education" or "economic policy". To test for this assumption with our sample of German Internet users, we asked respondents to rate the importance they attach to the topics listed in Figure 1 - the first question of our survey. To reduce immediate privacy priming, seven "filler" items have been added. We notice that German students attach considerable importance to privacy, which ranks second in importance: There is no significant mean difference between importance attached to Sustainability (*Nachhaltigkeit*), Environmental Protection (*Umweltschutz*) and Privacy in the Internet (*Datenschutz im Internet*). Similar to US respondents, "Education" (*Bildung*) emerges as the topic of higher importance (p-value=0.000), which is not surprising since most respondents were students. In contrast to US consumers, however, privacy issues outrun in importance major topics such as the Economy (*Wirtschaft*), as well as the EU Financial Crisis and Future of the Euro (*EU Finanzkrise und Zukunft des Euros*) for German respondents.

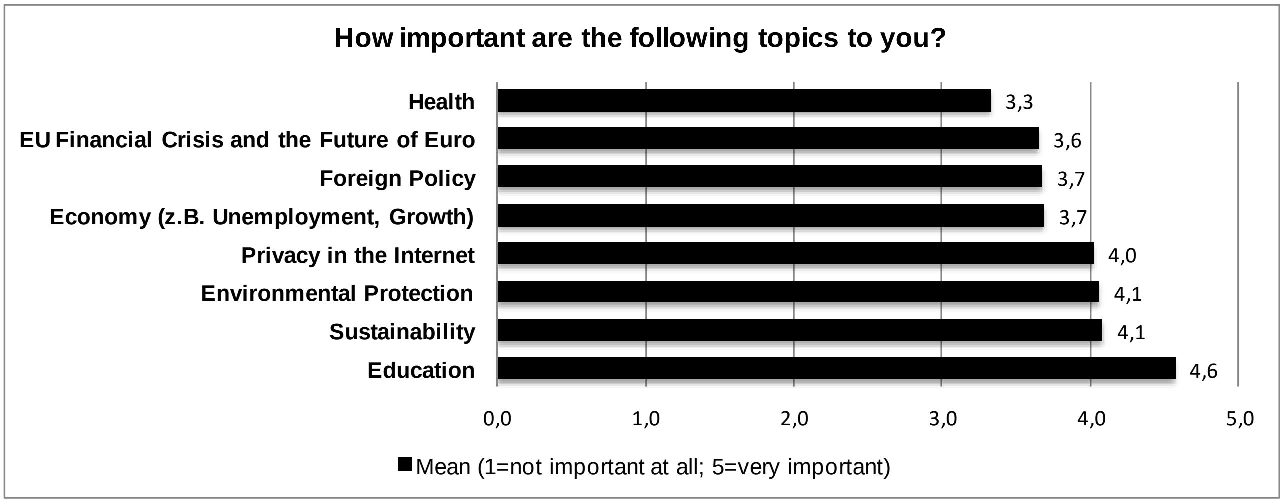

Figure 1: Importance of Privacy Topics

Furthermore, we register no significant gender differences in the importance attached to privacy. As for other issues, female users in our sample attach higher importance to Education (*Bildung*) (p-value=0.030) and Health (*Gesundheit*) (p=0.002), with male users being more interested in the EU financial crisis and the Future of the Euro (*EU Finanzkrise und Zukunft des Euros*) (p-value=0.012).

WHAT PRIVACY CONCERNS DO USERS HAVE?

A number of classifications for privacy concerns have been suggested. Recognizing the vast potential of organizations to collect and store consumer information using IT-enabled infrastructures, Smith et al. (1996) developed a taxonomy of concerns for information privacy (CFIP), in which they differentiate between four dimensions of individuals' concerns about organizational information privacy practices. Among them, the (1) *concern about information collection* reflects user anxiety about "*extensive amounts of personally identifiable data being collected and stored in databases*"; unauthorized secondary use represents the "*concern that information is collected from individuals for one purpose but is* *used for another, secondary purpose (internally within a single organization) without authorization from the individuals*"; (3) *improper access* reflects the "*concern that data about individuals is readily available to people not properly authorized to view or work with this data*"; and the (4) concern about *errors* reflects the anxiety that "*protections against deliberate and accidental errors in personal data are inadequate*" (Smith et al. 1996, p. 172).

To better target Internet context, Malhotra et al. (2004) develop a different classification of privacy concerns - Internet Users' Information Privacy Concerns (IUIPC). They argue that user privacy concerns are rooted in the perceptions of distributive, informational and procedural justice. Mapping these justice dimensions to the Internet privacy context, the authors distinguish between concerns over (1) *collection of information*, (2) *awareness* and (3) *control*. While operationalization of the *collection* dimension is similar to that of Smith et al. (1996), *control* is "*manifested by the existence of voice (i.e., approval, modification) or exit (i.e., opt-out)*". *Awareness*, in turn, reflects "*the degree to which a consumer is concerned about his/her awareness of organizational information privacy practices*" (Malhotra et al. 2004, p. 339).

Taking a deeper look at the concerns voiced by SNS users, Krasnova et al. (2009a) find that while users report being concerned about a large variety of threats, cognitively users place these concerns into two categories. The first category - *Concerns about Organizational Threats* - combines all concerns that users have related to the organizational use of their information. The study shows that users *neither* subjectively differentiate between *who* collects and uses the information they provide (SNS Provider vs. Third Parties) *nor* do they make a distinction between the *collection* and the *secondary use* of their information. In fact, secondary use by organizations is largely impossible without information collection, and therefore users may assume that a party collecting their information would also *use* it at some point. The second category - *Concerns about Social Threats* - is mainly related to the risks stemming from the SNS user environment. The authors find that individuals do not make distinctions based on the nature of the threat (purposeful bullying vs. involuntary uncontrollable actions of others), and concentrate on the source of the threat (social environment) instead.

To gain a better understanding of the magnitude and nature of privacy concerns in the general Internet context and on Facebook, respondents were asked a number of closed and open-ended questions. First, the magnitude of privacy concerns has been elicited via the following question: *Are you concerned about your privacy when using Internet / Facebook?* Pre-specified answers ranged from *1=not concerned at all; 2=hardly concerned; 3=moderately concerned; 4=very concerned; 5=extremely concerned* as summarized in Figure 2.

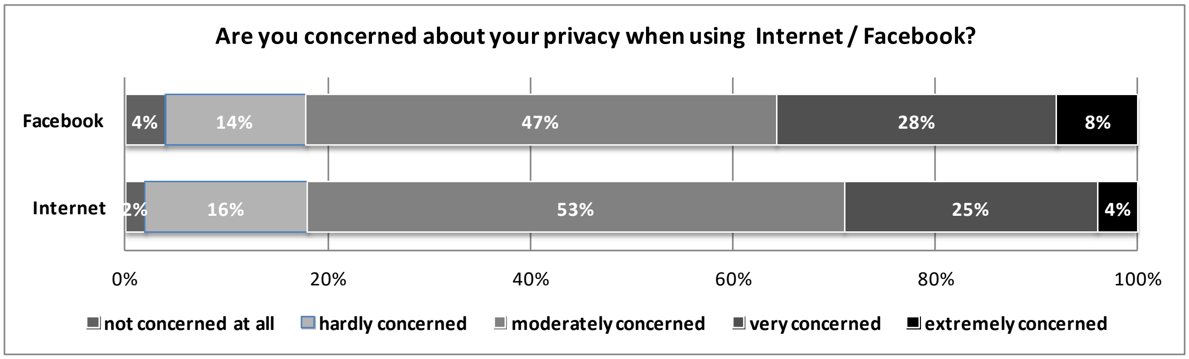

Figure 2: Magnitude of Privacy Concerns when using Internet and Facebook

Even though Facebook use is only a sub-part of the general Internet use, respondents expressed a higher degree of concern when using *Facebook* (mean=3,22) than when using the *Internet* (mean=3,13), with this difference being statistically significant (p=0.000). These answers suggest a logical inconsistency, which suggests that users associate *different types of threats and, as a consequence, have different concerns* when using the Internet and Facebook.

To better understand these differences users were asked two open questions: (1) "*Are you concerned about your privacy when using Internet? If yes, then why? If no, why not?"* and (2) "*Are you concerned about your privacy when using Facebook? If yes, then why? If no, why not?*" Open-ended questions are generally a preferred method to capture the nature and sources of privacy concerns, since they do not prime respondents on specific topics, but rather elicit immediate “top-of-mind” answers, which are likely to be more honest and reliable (Harper and Singleton 2001; Paine et al. 2007). The obtained data corpus of textual answers, comprising 9828 and 6826 words for Internet and Facebook questions respectively, served as a basis for the subsequent content analysis. Following methodological guidelines suggested by Ryan and Bernard (2000), we derived a preliminary set of themes (categories) relating to privacy concerns using existing theoretical insights. In addition, by in-vivo coding the material in an iterative manner, further categories were identified. While extracting a large number of categories may have complicated both analysis and interpretation, this approach was preferred to reflect the richness of the obtained data. Altogether the data was coded according to *five* major axes: *Type of Data* (see Figure 4), *Type of Threats* (see Figure 5), *Source of Threat (*see Figure 6*)*, *Data Control* (see Figure 7) and *Privacy Management Strategies* (see Figure 8). Figures 3-7 summarize the share of respondents mentioning a particular “code” in their answers. Appendix A provides an in-depth explanation and examples of quotations for each category.

When it comes to the *type of data* (Figure 3), we notice that users are mainly concerned about the misuse of their *personal data*, such as name, address, phone number, gender, birth date and photos. In contrast, theft of passwords or bank data was mentioned less often.

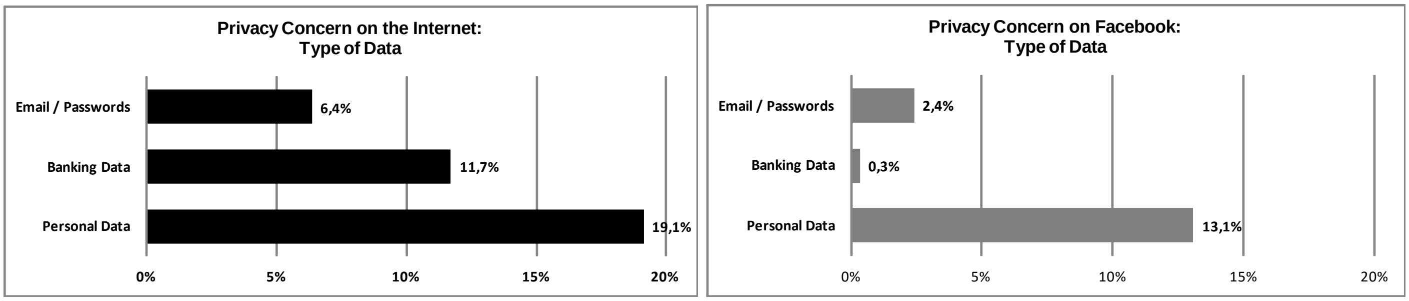

Figure 3: Privacy Concerns: Data Type

When discussing different *types of threats*, participants were often vague about what exactly they were concerned about, with a generic category “*data misuse*” emerging as the highest in importance for the Internet context (21,3%) (Figure 4). Apparently, not only policy-makers and scholars have a hard time arriving at a comprehensive definition of privacy, but users themselves often have mixed feelings about what constitutes a specific threat to their privacy. As a result, their demands for “more data protection” are often difficult to interpret and, hence, to address. Respondents, however, were more specific about their use of Facebook, with threats related to the “*unauthorized access to data”* (19,7%) and “*data dissemination”* (18,3%) emerging as the highest in importance. Evidently, Facebook users are on some level aware of the sensitivity of the information they disclose on SNSs as well as the damage publication of this information may entail.

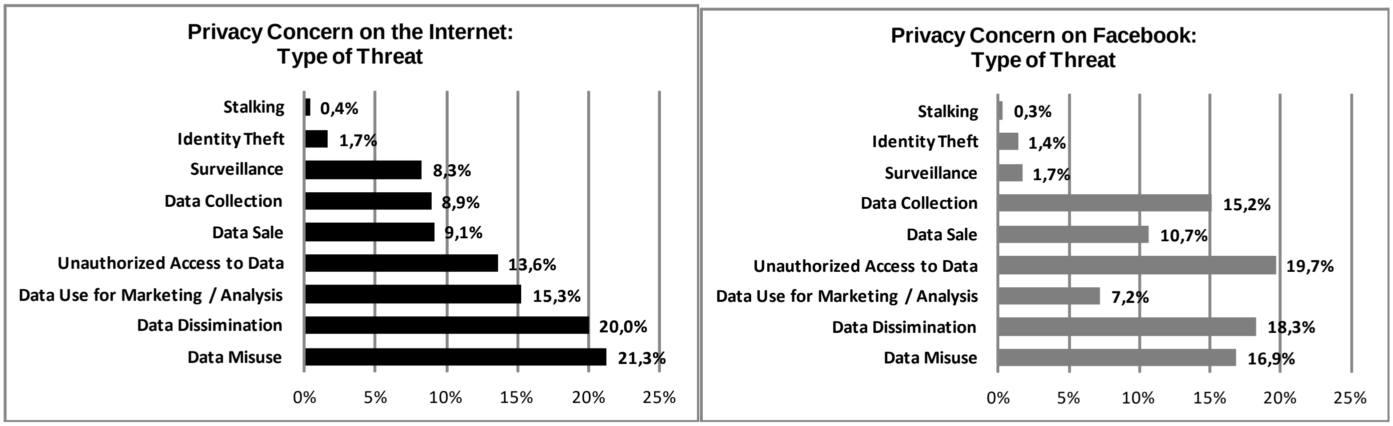

Figure 4: Privacy Concerns: Type of Threat

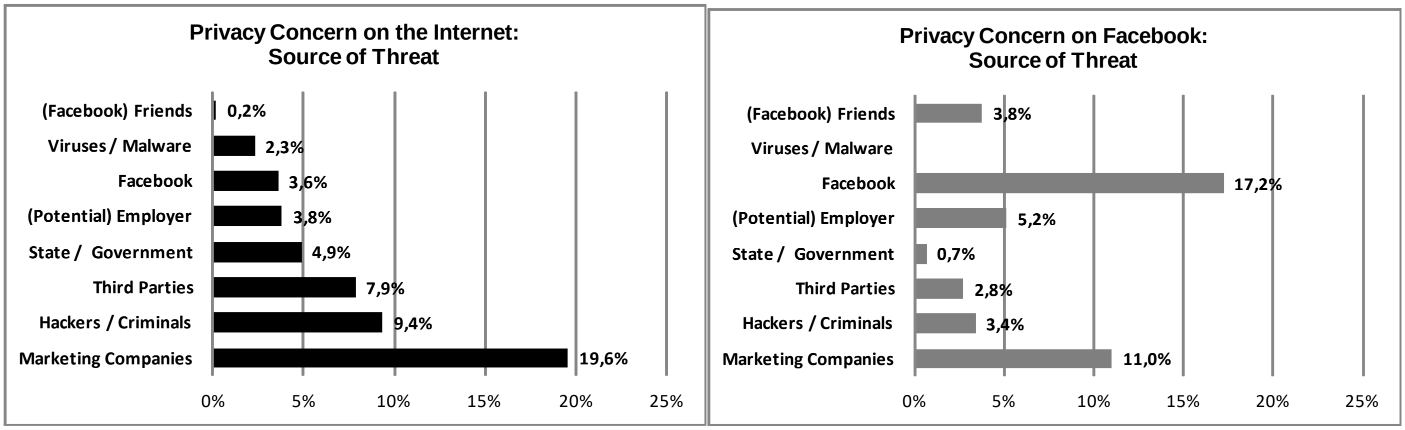

Figure 5: Privacy Sources of Threat

When it comes to specific *sources of threats* when using the *Internet*, *Marketing Companies* emerged as the category of the highest importance (19,6%) (Figure 5). They were followed by *Hackers and Criminals* (9,4%) and *Third Parties* (7,9%). Only few people mentioned *State / Government* (4,9%) as a particular source of threat to their privacy on the Internet. On Facebook, the situation was slightly different. Here, *Facebook* itself and *Marketing Companies* were seen as the highest sources of risk, with 17,2% and 11,0% of respondents mentioning these parties. Interestingly, only a meagre 0,7% of respondents mentioned *State / Government* as a threat to their privacy on Facebook.

Issues related to *the control* over one's information were frequently stated (Figure 6). Among them, respondents especially lamented a general *loss of control* (18,3) and *loss of privacy* (9,1%). It appears that, when asked about a general use of the Internet, respondents often lack concrete benchmarks upon which to base their concerns. Instead, a general vague feeling of anxiety is reported. For Facebook, respondents were able to come up with more specific answers, particularly resenting their *inability to* irrevocably *delete data* they provide on Facebook (8,3%) and the related *longevity of information* they share (9,0%).

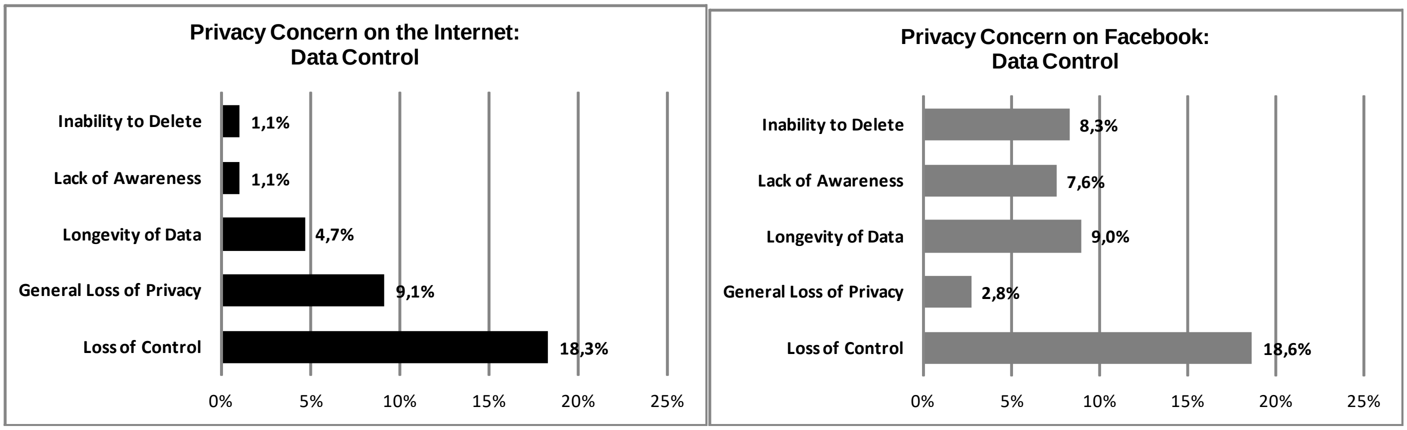

Figure 6: Privacy Concerns over Loss of Control

Finally, users reported a variety of strategies they employed in order to counteract privacy concerns (Figure 7). Since continuous concern may be self-destructive (Janof-Bulman and Lang-Gunn 1988), respondents sought out ways to regain their confidence when using Internet and Facebook. Specifically, 14,9% of the Internet sample and a whopping 34.5% of the Facebook sample mentioned to consciously *self-control information they publish*. A small, but nonetheless, significant share of respondents (11,5% of the Internet and 8,3% of the Facebook sample) adopted a specific anxiety-reducing attitude, as they claimed to "*not care*" about privacy, since they had "*no choice*" and "*nothing to fear*", or "*were not important*" or "*interesting*" enough for their data to be relevant to anyone. Interestingly, the use of technical means or simple anonymization was only marginal mentioned.

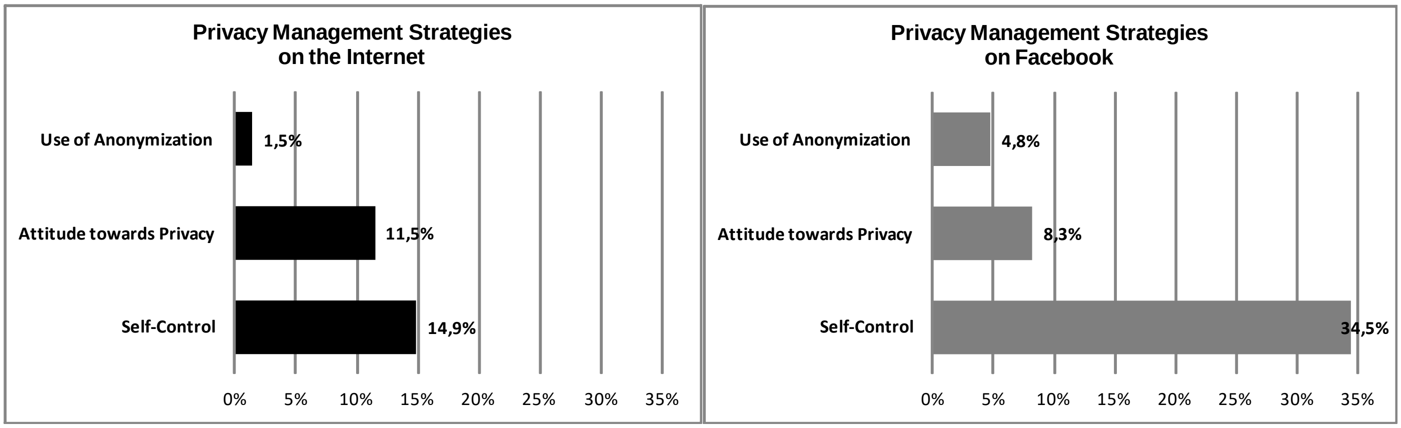

Figure 7: Privacy Management Strategies

Overall, results reported in Figure 5 suggest that users in our sample felt more threatened by *private parties* such as Facebook or marketing companies than by the state/government. The reason for this could be that respondents attributed a higher likelihood to threat emerging from these sources (Krasnova et al. 2009c). This finding was additionally confirmed by responses to the following question: *"How much do you trust these parties not to abuse your data?"* with answers ranging from *1=do not trust at all*; to *4=trust very much*. As demonstrated in Figure 8, our analysis suggests a similar picture: Respondents felt that their data was generally safe with state organizations such as the *police* and *state authorities*, to whom they attributed a *moderate degree of trust*. In contrast, respondents were distrustful of private parties, with *Amazon* being the most trusted commercial organization, followed by *Google* and finally *Facebook*. Overall, European consumers have been consistently found to be more trustful of the government than of commercial parties (Samuelson 2008). Whether or not users of different cultural backgrounds also hold these beliefs should, however, be verified in future studies.

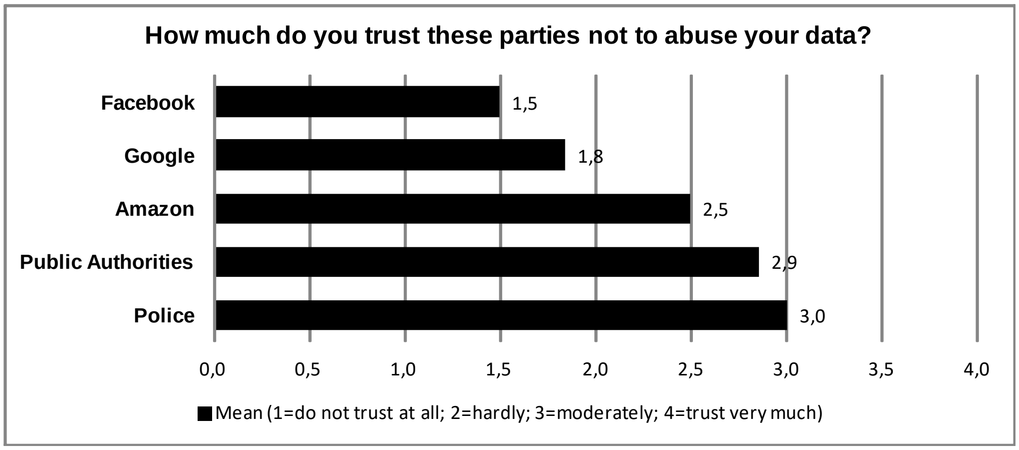

Figure 8: Trust in Different Parties

THE ROLE OF PRIVACY CONCERNS IN PRIVACY BEHAVIOR

Whether and how stated privacy concerns impact actual behaviour is the subject of a heated debate. While users consistently report high level of privacy concerns, their behaviour is in contradiction to their expressed fears. For example, the sheer size of information sharing registered on Facebook is, at first glance, inconsistent with the magnitude of privacy concerns reported (see Figure 2). Similarly, in the online shopping context, Spiekermann et al. (2001) show that users who claim to be highly concerned about their privacy online – privacy fundamentalists – still have a strong tendency to self-disclose their identity information and other preferences to an online recommendation agent for no apparent reason. Exhibiting similar inconsistencies, multiple sources document a low actual rate of "cookie" rejection, low attention to privacy policies, and lack of demand for “privacy” hotlines (Harper and Singleton 2001, Federal Trade Commission 2001). For example, Ted Wham – a former Chief Privacy Officer of Excite@Home - reported that less than 100 out of 20 million visitors accessed their privacy policy immediately following an extensive TV coverage on the privacy risks of this particular web-site (Federal Trade Commission 2001). State-of-the-art research offers a number of competing explanations for the observed phenomenon, as discussed below.

Privacy Calculus

Privacy Calculus theory suggests that users act as rational agents when it comes to privacy. They are expected to carefully weight risks and benefits of their self-disclosures and act in line with their preferences (Dinev and Hart 2006). Indeed, privacy is by far not the sole factor in one’s decision to reveal information. For example in the online context, Hui et al. (2006) differentiate between two groups of benefits that induce users to share. On the one hand, *extrinsic benefits* such as the desire to save time and money, as well as gaining the benefits of self-enhancement and social adjustment induce users to act in disaccord with their asserted privacy interests. On the other hand, *intrinsic benefits* such as experiencing pleasure, novelty and altruistic feelings motivate users to self-disclose online. Providers of online shopping platforms readily use these motivational triggers in an attempt to learn more about users’ demographics, preferences and behavioural patterns. In the SNS context, self-disclosure is typically associated with benefits such as self-enhancement, information exchange and self-expression, relationship maintenance, and pastime (Krasnova et al. 2010a; 2010c Koroleva et al. 2011).

To gain a snapshot of driving forces behind users’ motivation to share on SNSs, an experiment has been integrated into our survey. Specifically, respondents were randomly assigned to one of the *two* experimental conditions. In the first condition, respondents were asked: “*Please think about the information you share on Facebook (e.g. status updates, photos, etc.). Why do you share this information?*” In the second condition, the same question was asked, but with respect to Facebook friends: “*Please think about the information your Facebook friends share on Facebook (e.g. status updates, photos, etc.). Why do they share this information?*” Respondents had to express the degree of their agreement to an array of motives pre-specified by the authors on a 5-point scale: *1=strongly disagree; 5=strongly agree*. The need for this projective experimental set-up was dictated by differences in social desirability of certain motivations (Donoghue 2000): While users may be willing to admit motivation “*to share relevant information*”, they may be reluctant to report desire “*to impress others*” when sharing. In this regard, asking respondents about “*their friends*” might be a better indicator of what motivated respondents themselves.

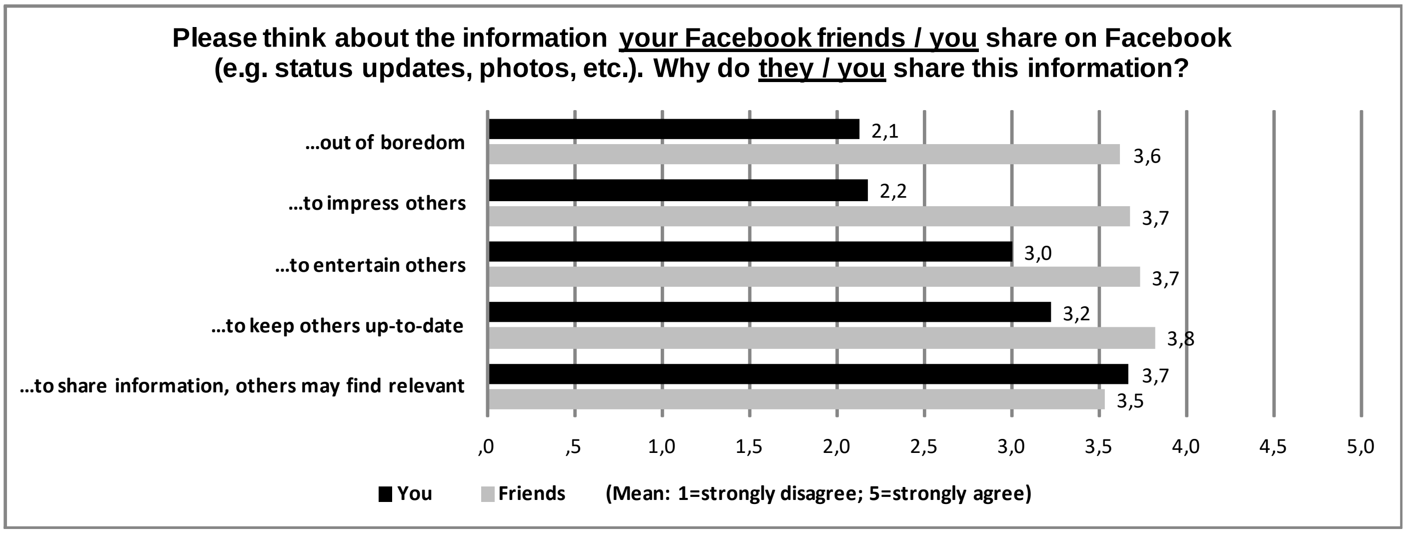

Figure 9: Motivation to Share Information

Figure 9 provides a summary of the responses. We find that when reporting either about *themselves* or *their friends*, respondents have chosen the desire to broadcast “*relevant information”* and to “*keep others up-to-date”* as the main motivations behind their sharing activity. Respondents were unwilling to admit sharing information "*out of boredom"* or to "*impress others"*. In contrast, these "socially undesirable" motives were often attributed to "friends". In fact, we find no significant mean difference between various motivations of "friends", except for "*sharing information relevant to others"*.

Altogether, users face certain trade-offs when deciding whether or not to reveal information. Actual decisions they make in these choice situations may shed light on the real value users attach to privacy. As mentioned above, in the past the value users attach to privacy has often been elicited using survey data. However, Harper and Singleton (2001, p.2) argue that privacy surveys "*suffer from the 'talk is cheap' problem*", since it costs respondents nothing to claim their concern for privacy. Moreover, respondents may feel that admitting privacy concerns is expected of them and is also socially desirable. As a result, limited conclusions can be derived from the choices respondents would make when facing trade-offs between privacy and other competing interests. To address these constraints, a limited number of studies have adopted elaborate techniques to measure and, more importantly, monetize the value users attach to their privacy. Among them the use of the conjoint analysis represents one of the most appealing methods. In experiments involving conjoint analysis, respondents have to make real choices between an array of previously developed "trade-off" scenarios. Examples include: "Provider uses your information, but SNS is for free" vs. "Provider does not use your information but SNS use costs €5 a month". Outcomes of conjoint analyses shed light on real user preferences. For example, investigating Facebook use, Krasnova et al. (2009b) find that while on average users do attach value to their privacy, there are striking discrepancies between different user clusters. Specifically, the authors derive 3 types of user groups: "*Unconcerned Socializers*" - predominantly young male, who attach little value to privacy and are also not willing to pay for it. "*Control-conscious Socializers*" - predominantly female - who place great value on being able to selectively control their self-disclosure. And "*Privacy Concerned*", who would be willing to pay €1.928 – €2.348 a month to ensure that a provider does not use their demographic information.

While conducting conjoint analysis was out of the scope of this study, we have undertaken the first step in measuring the *monetary value users attach to privacy*. Indeed, willingness to pay for privacy is one of the critical indicators of the value users attach to it. Moreover, monetary savings are a frequent cause to reveal one's information to retailers and marketers as part of customer card programs (Hui et al. 2006). Two direct questions have been posed. For the general Internet context, respondents were asked: "*How much in taxes would you be willing to pay per month to ensure that policy-makers engage themselves with the topic "privacy" more intensively?"* For Facebook context, the question was phrased in the following way: "*Some people are concerned that the information they share on Facebook is not adequately protected and can be used for other purposes (e.g. personalized advertisement). How much would you be willing to pay to Facebook per month to avoid that?"*. Table 3 and Figure 10 summarize obtained results.

Table 3: Willingness to Pay for Privacy

Statistics	**Per Month in Taxes, n=457**	**Facebook, n=379**
Mean (with Outliers)	6,4 €	0,78 €
Trimmed Mean (w/o Outliers)	**4,3 €**	**0,29 €**
Median	2,0 €	0,0 €
Minimum	0,0 €	0,0 €
Maximum	100,0 €	25,0 €
Std. Deviation	12,6 €	2,8 €
Range	**Frequencies**	**Frequencies**
0 €	34,4%	79,4%
More than **0** and less or equal to **2 €**	17,3%	12,7%
More than **2** and less or equal to **5 €**	22,8%	5,5%
More than **5** and less or equal to **10 €**	14,4%	1,1%
More than **10** and less or equal to **20 €**	6,1%	0,8%
More than **20** and less or equal to **100 €**	5,0%	0,5%

We find that, on average, users are willing to pay 4.3€ in taxes to ensure more policy-making in the area of privacy. These results are in stark contrast to Facebook, for which users are only willing to pay an average of 0,29 € a month (trimmed mean values). In fact, while only 34.4% were *not* willing to pay any amount in taxes for more policy-making, this figure reached a whopping 79.4% for Facebook. There are multiple explanations for the observed phenomenon. Users may be doubtful that Facebook is actually willing to protect their privacy, as shown in Figure 5. Furthermore, users might not be as accustomed to pay for SNS services as they are to paying taxes. In addition, Facebook users may believe that even if Facebook took greater efforts to protect their privacy online, accessibility of their information to Facebook friends would continue rendering their information difficult to protect.

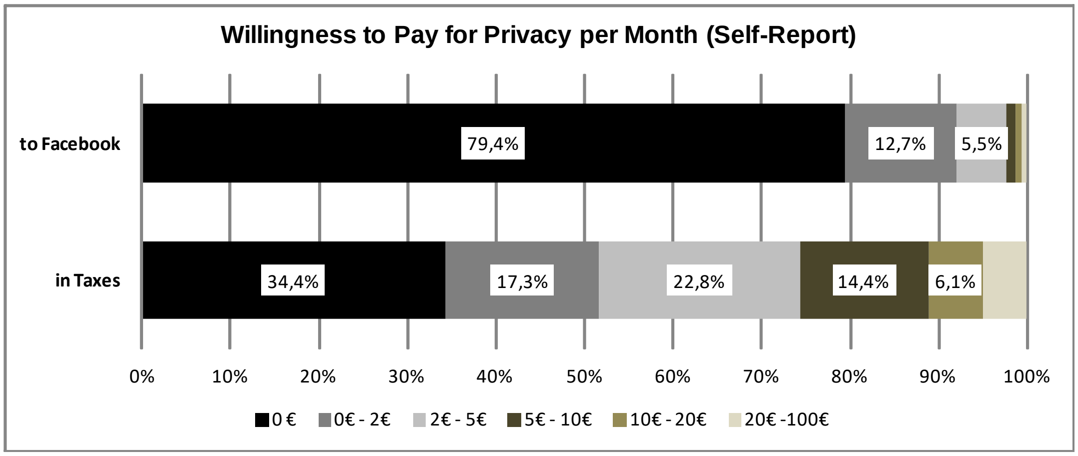

Figure 10: Willingness to Pay for Privacy

All in all, the willingness respondents expressed to pay more taxes in order to ensure adequate privacy protection underscores the salience of privacy concerns in individual decision-making.

Cognitive Distortions

Another line of research offers an alternative explanation for the observed discrepancy between privacy concerns and user behaviour. Thus, Acquisti (2004) argues that even in situations where users are willing to consciously filter their self-disclosure, they are unlikely to make optimal decisions due to inherent cognitive limitations. Indeed, bounded rationality, incomplete information, hyperbolic discounting and similar aberrations hardly make privacy decisions a matter of rational choice (Acquisti 2004). For example, in a set of experiments, John et al. (2009) demonstrate that simple changes in question formulations or survey visual design can lead users to reveal details as sensitive about themselves as drug consumption, plagiarism, unusual sexual practices, and cases of cheating both on exams and in a relationship. Cognitive limitations may also explain a widespread reliance on "*defaults*". Indeed, when it comes to such complex matters as privacy, people tend to rely on simplifying heuristics to make a choice (Acquisti 2004). In this case, relying on default settings suggested by a provider seems to prove the most natural, but not necessarily the best, strategy at their disposal (Ariely 2008).

Optimistic bias or "*It won't happen to me!*" attitude represents another common type of cognitive distortion. Due to optimistic bias, individuals tend to perceive negative events as less likely and positive events as more likely to happen to them (Higgins et al. 1997). This phenomenon can been observed in many aspects of human behaviour including Internet events (Campbell et al. 2007) and information sharing on Facebook (Krasnova et al. 2009c). The reasons for these distortions include egocentricity, focus on the base-rate information and a variety of motivational causes (e.g. Higgins et al. 1997).

To indirectly test for the presence of these effects, we have asked respondents *how likely they would follow up on the changes in Facebook's privacy policy and privacy settings*, with pre-specified options ranging from: *1=very unlikely; 2=unlikely; 3=likely; 4=very likely*. Summarized in Figure 11, we find that more respondents were *(very) unlikely* to follow up on *privacy policy* as opposed to *privacy settings* (p-value=0.003). The reason could be that respondents considered themselves unable to understand the complex legalistic language and more important legal implications of the introduced changes. Most interesting however, is the lack of a significant correlation between the willingness to follow up on the changes (in both privacy policy and privacy settings) and stated privacy concerns (described in Figure 3), which may be interpreted as (1) the respondents' subjective lack of ability to understand the implications of the introduced changes and (2) the presence of optimistic bias and similar distortions.

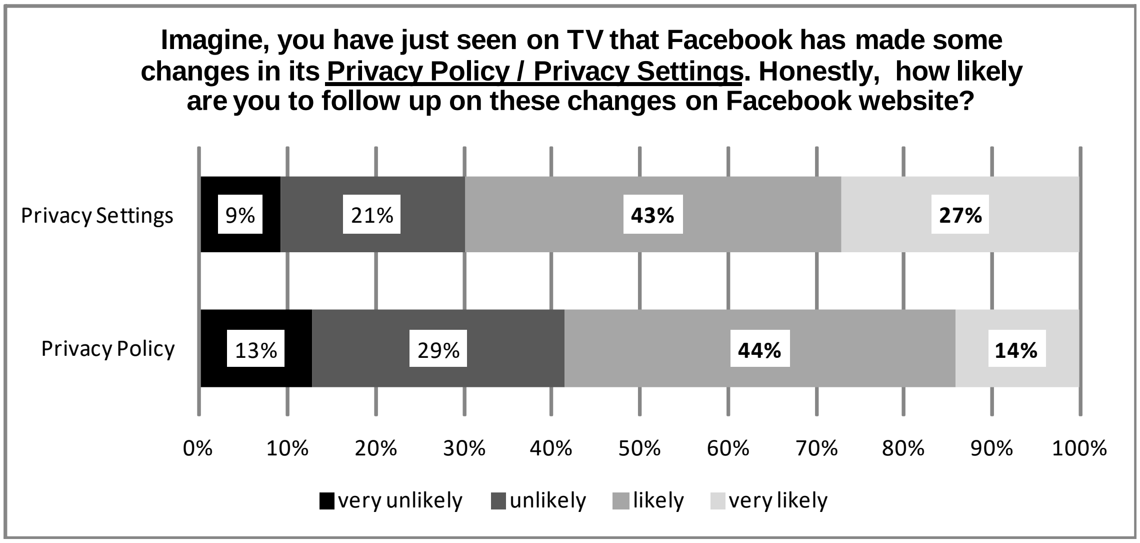

Figure 11: Following on the Changes in Privacy Policy and Privacy Settings

DO USERS RELY ON LEGAL ASSURANCES TO MITIGATE PRIVACY CONCERNS?

As perceptions regarding privacy risks are situational, they are likely to be influenced by the institutional structures inherent to the environment (Grabner-Kräuter and Kaluscha 2003). Indeed, even in situations when users put their privacy at risk, they can still accept the presence of risks "*because of structures, situations, or roles that provide assurances that things will go well*" (McKnight and Chervany 2001-2002, p. 46). Recognizing their pivotal nature in addressing privacy needs of online consumers, McKnight et al. (2002a; 2002b) differentiate between two components of structural assurances: legal and technological. Whereas technological assurances (such as firewalls or encryption) are increasingly standardized across the web, privacy laws diverge immensely from one country to another. For example, privacy regulation is largely industry-specific in the USA. Germany, on the other hand, has a comprehensive legal framework that covers numerous aspects of personal data access, collection and use. These differences might, therefore, be able to account for a lower level of privacy concerns expressed by German subjects as opposed to U.S. subjects (Krasnova et al. 2010b), despite a much higher level of uncertainty avoidance of German society (Hofstede 2001). Against this background, we take a closer look at the role of legal assurances – privacy-related laws, legally-enforced policies and procedures – in the dynamics of privacy concerns.

In the theoretical discourse, opinions on the role of legal assurances in mitigating privacy concerns and influencing consumer trust remain mixed. On the one hand, investigating the organizational context, Sitkin and Roth (1993, p. 367/369) argue that legalistic remedies, such as formal rules, sanctioning or contracts, are ineffective in restoring interpersonal trust between employees and management. In their view, increasing regulation creates psychological and interactional barriers, which lead to a vicious cycle of perpetually increasing formality and distance. On the other hand, IS-researchers agree that a sound legal framework may help to create an atmosphere of trust on the platform (McKnight et al. 2002a; 2002b). Particularly, when a relationship is associated with significant risks, the mechanism of institution-based trust works to create a much needed "*trust infrastructure*" (Lou 2002). Beyond their impact on trust, perceptions regarding legal assurances are likely to give users more confidence when it comes to privacy and security of their data (McKnight and Chervany 2001-2002, p. 46). In the absence of obvious means to control the use of personal information, particularly by providers, legal assurances are likely to be the best solution to privacy concerns (Lou 2002). Hence, it comes as no surprise that SNS providers are increasingly relying on third party seals to gain credibility in the eyes of their users: while Facebook boasts TRUST and EU Safe Harbor seals, StudiVZ has placed four privacy-relevant seals on its website. By presenting these privacy guarantees, SNS providers signal that their information-handling practices comply with the required standards. The importance of legalistic means for mitigating privacy concerns is also supported by privacy control models, which view legal authorities as mediators between a data-source and data recipient (Pincus and Johns 1997).

To further explore the role of legal assurance in the context of our study, we asked respondents whether existing legal assurances present in Germany offer an effective protection for their Internet and Facebook use, with pre-specified answers ranging from: *(1)=absolutely not; (2) rather not; (3) yes, to some extent; (4) yes, absolutely*. We find that respondents felt more protected when using Internet in general than when using Facebook (p-value=0.000). Overall, however, the level of reliance on legal assurances was low, with an overwhelming 82% and 72% arguing that the existing legal framework either offers *absolutely no protection* or *hardly any protection* for Facebook and Internet users, respectively (see Figure 12).

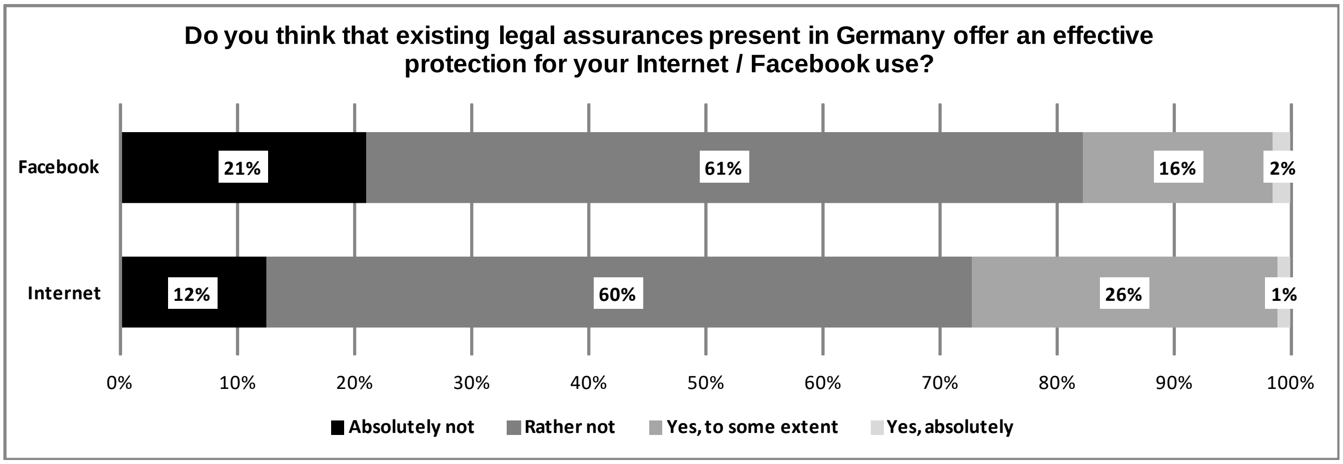

Figure 12: Effectiveness of Legal Assurances in Germany

To better understand the rationale behind these sentiments, respondents were asked to comment on why (or why not) they attributed a certain level of effectiveness to the legal framework in Germany. Specifically, two open questions were asked: (1) "*Do you think that existing legal assurances present in Germany offer an effective protection to Internet users? If yes, why? If no, why not?*" and (2) "*Do you think that existing legal assurances present in Germany offer an effective protection to Facebook users? If yes, why? If no, why not?*". The obtained data corpus of textual answers, comprising 7950 and 4670 words for Internet and Facebook questions respectively, served as a basis for the subsequent content analysis. Similar to the procedure described above, we used theoretical insights and in-vivo coding to identify a set of reasons (categories) for a reported sentiment. Altogether the data was coded across two major axes: "Why is the legal framework ineffective?" and "Why is the legal framework effective?". Figures 13 and 14 summarize the share of respondents mentioning a particular "code" in their answers. Appendix B provides examples of quotations for each particular code.

We find that the "*inability of laws to cover everything*" is mentioned as one of the key reasons for the ineffectiveness of legal frameworks applied to the Internet (36% of respondents) and to Facebook (25% of respondents). This reason goes hand in hand with the fact that "*technological advances outpace legal regulation*" (17% / 8% of respondents for the Internet and Facebook respectively) and the "local character of laws" (17% / 28% of respondents for the Internet and Facebook respectively). In fact, the "*local character of laws*" was the most mentioned reason for the ineffectiveness of legal assurances in protecting Facebook users (28% of respondents). Interestingly, the reason that "*Facebook has power*" emerged as the third most mentioned code within the Facebook context, with respondents often commenting that Facebook can do what it wants in any case: "*Facebook hat zu viel Macht und der Staat hat nicht genug Einfluss auf Facebook, um einen passenden Datenschutz durchzusetzen*" (quotation in German). To our surprise the topic of lacking awareness ("*I do not know which laws exist*") did not emerge as a salient factor, being mentioned by only 9% and 7% of Internet and Facebook users respectively. Apparently, users (believe to) have a certain understanding of how their privacy is protected. We do not, however, preclude that these beliefs can be erroneous.

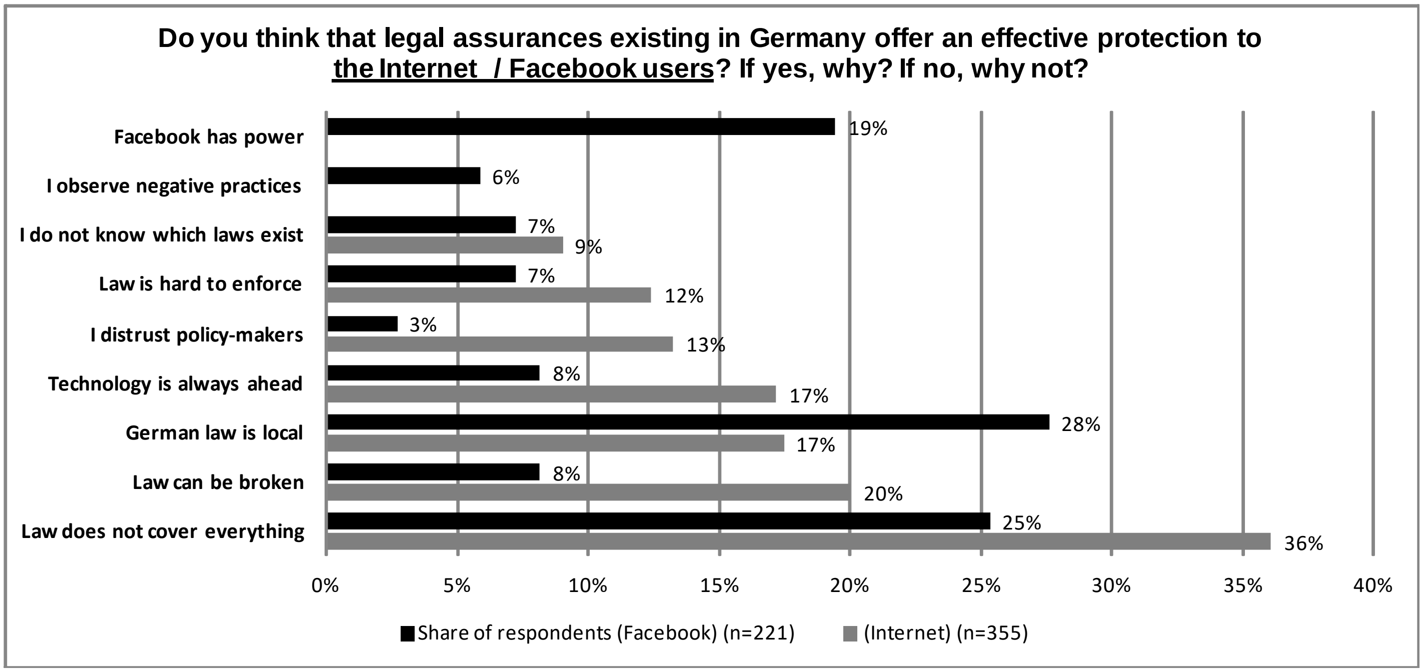

Figure 13: Why is Legal Framework Ineffective?

While 36% of respondents believed that existing laws "*do not cover everything*" when it comes to the Internet use (Figure 13), 14% of respondents argued that the law offers "*at least some protection*", especially because there are "*strong German laws*" (5% of respondents) (Figure 14). Finally, some users did not desire more legal regulation, since they assumed that privacy was the responsibility of users - a rationale particularly common to Facebook users (7% of respondents) (Figure 14). Again, it appears that Facebook users are on some level aware that they themselves are responsible for their privacy when it comes to the use of SNSs. Reasons include voluntary nature of information sharing on Facebook, as well as users' ability to at least determine accessibility, with regard to their social circle.

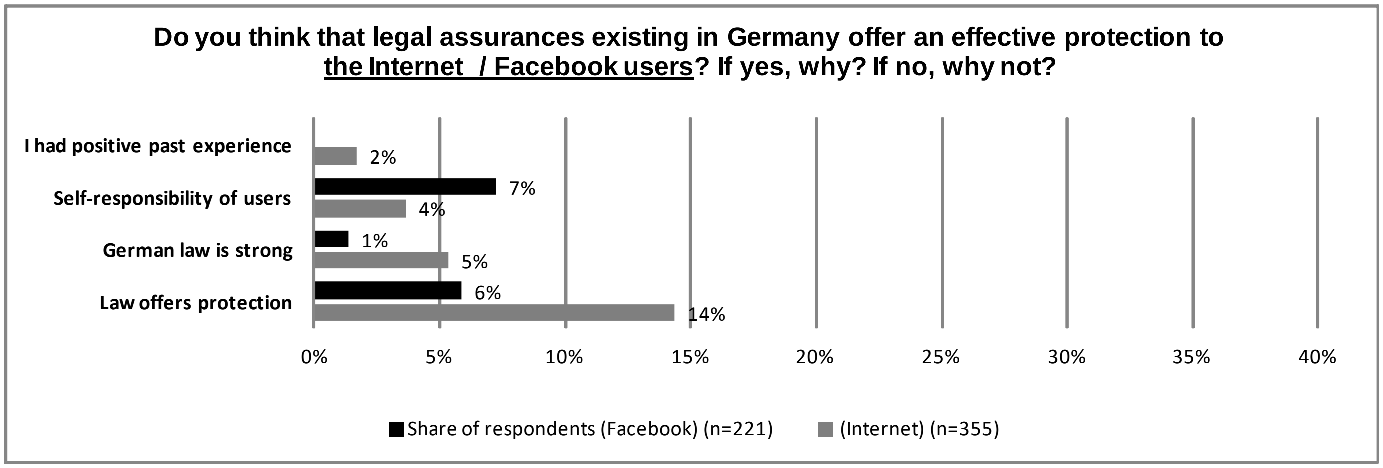

Figure 14: Why is Legal Framework Effective?

Finally, we asked respondents to comment on the likelihood of changes in legal regulations to affect their sharing behaviour on Facebook: "*Imagine policy-makers have adopted stronger laws to protect your data on Facebook. Will you share more or less on Facebook following these changes (e.g. status updates, photos)?*" with pre-specified answers: *(1)*

the same as before; (2) a little bit more; (3) more; (4) much more. We find that an overwhelming share of respondents (83%) did not expect to alter their behaviour in response to these changes (see Figure 15). The rationale behind these results can be traced back to the reasons summarized in Figure 13. With Facebook and other SNSs being on the market for over 8 years already, users appear to have developed individual strategies to manage and protect their privacy. According to our results, positive changes in the legal assurances are unlikely to be a decisive trigger for these strategies to be reconsidered.

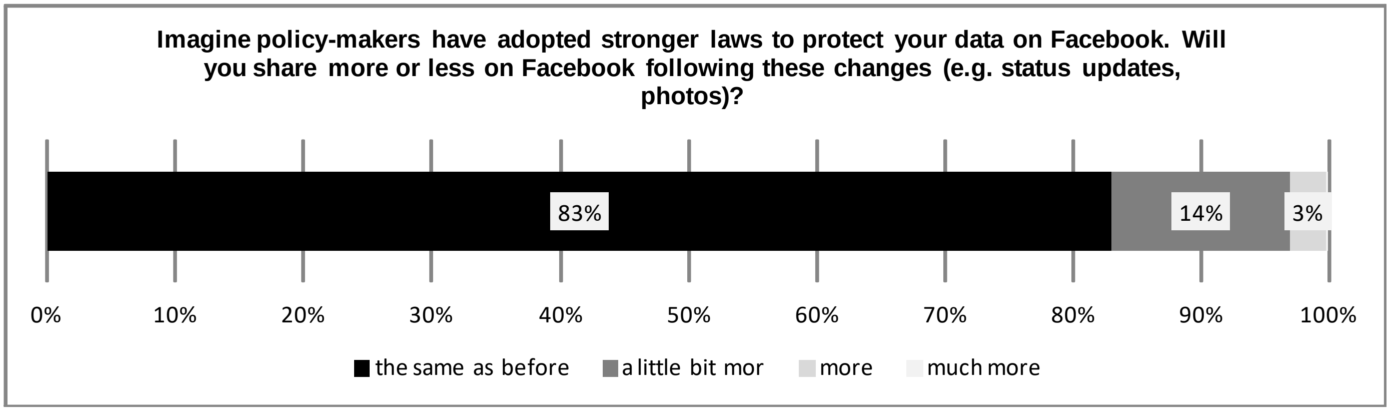

Figure 15: Impact of Stronger Legal Assurances on User Behavior

CONCLUDING REMARKS

Based on a sample of 553 respondents, our findings suggest that users have a complex attitude towards privacy issues and the regulation thereof. On the one hand, users tend to express strong concerns about privacy when asked directly. At the same time, users often have difficulties formulating the exact nature of these concerns, with Internet users often lamenting data misuse, as well as a general loss of control over data and privacy. In the Facebook context, Facebook is often mentioned as the primary source of threat, closely followed by marketing organizations. All in all, commercial providers, such as Facebook, are viewed with distrust. In contrast, public authorities and other state organizations are considered trustworthy. Despite these stated concerns, the desire of users to counteract them remains limited. Possible reasons include privacy calculus as well as numerous cognitive distortions. Apparently, an array of benefits associated with self-disclosure outweighs perceived risks on numerous occasions.

In terms of legal assurance, users feel little protected by the existing legal framework, due to a common belief that the law is unable to address the complexity of the Internet and SNS phenomenon, as well as due to the local character of laws, and the deeply-rooted belief that even when laws are present, others may not necessarily follow them, particularly since enforcement is difficult to achieve. This ambiguity with regard to legal protection is particularly pronounced within the Facebook context. With a tendency to disregard legal assurances within their “privacy calculus equation”, users develop individual self-disclosure strategies to manage and protect their privacy. For some, responsible information sharing online represents the best strategy to protect against privacy abuse. Overall, according to our results, positive changes in the legal assurances are unlikely to be a decisive trigger for these strategies to be reconsidered.

As for limitations, our findings are based on a sample of predominantly German students. In future studies, respondents of different educational and cultural backgrounds and various ages may be surveyed in order to obtain a more comprehensive picture.

REFERENCES

Acquisti, A., and Gross, R. 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," in *Privacy Enhancing Technologies: 6th International Workshop, PET 2006, Cambridge, UK, June 28-30, Revised Selected Papers*, G. Danezis and P. Golle (eds.), Cambridge, UK: Springer-Verlag, pp. 36-58.

Acquisti A. 2004. "Privacy in Electronic Commerce and the Economics of Immediate Gratification," *EC '04 Proceedings of the 5th ACM conference on Electronic commerce*, New York, NY: ACM, pp. 21-29.

Alexa.com. 2012. "Statistics Summary for facebook.com," *Alexa: The Web Information Company*, http://www.alexa.com/siteinfo/facebook.com, last accessed August 23, 2012.

Ariely, D. 2008. *Predictably Irrational: The Hidden Forces That Shape Our Decisions*, New York, NY: Harper Collins.

Campbell, J., Greenauer, N., Macaluso, K. and End, C. 2007. "Unrealistic Optimism in Internet Events," *Computers in Human Behavior* (23:3), pp. 1273-1284.

CVP Marketing Group. 2011. "Facebook Demographics Revisited – 2011: Statistics by Ken Burbary," http://www.facebook.com/note.php?note_id=197149076992338, last accessed August 23, 2012.

Dinev T. and Hart P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research*, (17:1), pp. 61-80.

Donoghue, S. 2000. "Projective Techniques in Consumer Research," *Journal of Family Ecology and Consumer Sciences* (28), pp. 47-53.

Federal Trade Commission. 2001. "The Information Marketplace: Merging and Exchanging Consumer Data," *Federal Trade Commission Public Workshop*, Washington, D.C., http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm, last accessed August 23, 2012.

Grabner-Kräuter, S. and Kaluscha, E. A. 2003. "Empirical Research in On-line Trust: A Review and Critical Assessment," *International Journal of Human-Computer Studies* (58:6), pp.783-812.

Harper J., and Singleton S. 2001. "With a Grain of Salt: What Consumer Privacy Surveys Don't Tell Us," *Competitive Enterprise Institute*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=299930, last accessed August 23, 2012.

Higgins, N. C., St Amand, M. D., and Poole, G. D. 1997. "The Controllability Of Negative Life Experiences Mediates Unrealistic Optimism," *Social Indicators Research* (42), pp. 299–323.

Hofstede, G. 2001. *Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations*, Thousand Oaks, CA: Sage Publications.

Hogben, G. 2007. "Security Issues and Recommendations for Online Social Networks," *ENISA Position Paper*, Heraklion: European Network and Information Security Agency, pp. 1-31.

Hui K.L., Tan B.C.Y., and Goh C.Y. 2006. "Online Information Disclosure: Motivators and Measurements," *ACM Transactions on Internet Technology* (6:4), pp. 415-441.

Janof-Bulman, R. and Lang-Gunn, L. 1988. "Coping with Disease, Crime, and Accidents: The Role of Self-Blame Attributions," in *Social Cognition and Clinical Psychology: A Synthesis*, L. Y. Abramson (ed.), New York, NY: Guilford, pp. 116–147.

John, L. K., Acquisti, A., and Loewenstein, G. F. 2009. "The Best of Strangers: Context Dependent Willingness to Divulge Personal Information," *Social Science Research Network*, http://ssrn.com/abstract=1430482, last accessed August 23, 2012.

Hampton, K. N., Sessions Goulet, L., Rainie, L. and Purcell, K. 2011. "Social Networking Sites and Our Lives," *Pew Research Center's Internet & American Life Project*, http://pewinternet.org/Reports/2011/Technology-and-social-networks.aspx, last accessed August 23, 2012.

Koroleva, K., Krasnova, H., Veltri, N. and Günther, O. 2011. "It's All About Networking! Empirical Investigation of Social Capital Formation on Social Network Sites," *ICIS 2011 Proceedings.*

Krasnova, H., Günther, O., Spiekermann, S., and Koroleva, K. 2009a. "Privacy Concerns and Identity in Online Social Networks," *Identity in the Information Society Journal*, Dordrecht: Springer Netherlands, http://www.springerlink.com/content/l371174132178uwm, last accessed August 23, 2012.

Krasnova, H., Hildebrand, T., and Günther, O. 2009b. "Investigating the Value of Privacy in Online Social Networks: Conjoint Analysis," *International Conference on Information Systems*, pp. 1-18.

Krasnova H., Kolesnikova E., and Günther O. 2009c. "It Won't Happen To Me!: Self-Disclosure in Online Social Networks," *15th Americas Conference on Information Systems*, San Francisco, CA: AMCIS, pp. 1-9.

Krasnova H., Spiekermann S., Koroleva K., and Hildebrand T. 2010a. “Online Social Networks: Why We Disclose,” *Journal of Information Technology* (25:2), pp. 109-125.

Krasnova H., and Veltri N. F. 2010b. “Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA,” *Proceedings of the 43rd Hawaii International Conference on System Sciences*, pp. 1-10.

Krasnova, H., Koroleva, K., and Veltri, N. F. 2010c. “Investigation of the Network Construction Behavior on Social Networking Sites,” *ICIS 2010 Proceedings*, Paper 182, http://aisel.aisnet.org/icis2010_submissions/182, last accessed August 23, 2012.

Kruglanski, A.W. 1975. “The Human Subject in the Psychology Experiment: Fact and Artifact,” in *Advances in experimental social psychology*, L. Berkowitz (ed.), New York, NY: Academic Press, pp. 101-147.

Luo, X. 2002. “Trust Production and Privacy Concerns on the Internet: A Framework Based on Relationship Marketing and Social Exchange Theory,” *Industrial Marketing Management* (31:2), pp. 111-118.

Malhotra, N. K., Kim S. S., and Agarwal, J. 2004. “Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model,” *Information Systems Research* (15:4), pp. 336-355.

McKnight D. H., Choudhury, V., and Kacmar C. 2002a. “Developing and Validating Trust Measures for E-commerce: An Integrative Typology,” *Information Systems Research* (13:3), pp. 334-359.

McKnight D. H., Choudhury, V., and Kacmar, C. 2002b. “The Impact of Initial Consumer Trust on Intentions to Transact with a Web Site: A Trust Building Model,” *Journal of Strategic Information Systems* (11), pp. 297-323.

McKnight, D. H. and Chervany, N. L. 2001–2002. “What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology,” *International Journal of Electronic Commerce* (6:2), pp. 35–59.

Paine, C., Reips, U. D., Stieger, S., Joinson, A. and Buchanan, T. 2007. "Internet users' perceptions of ‘privacy concerns’ and ‘privacy actions’," *International Journal of Human-Computer Studies* (65:6), pp. 526-536.

Pincus L. B., and Johns R. 1997. “Private Parts: A Global Analysis of Privacy Protection Schemes and a Proposed Innovation for Their Comparative Evaluation,” *Journal of Business Ethics* (16), pp. 1237– 1260.

Pring, Cara. 2012. “100 social media statistics for 2012,” *The Social Skinny: Get the Inside Scoop on All Things Social Media*, http://thesocialskinny.com/100-social-media-statistics-for-2012, last accessed August 23, 2012.

Ryan G. W., and Bernard H. R. 2000. “Data Management and Analysis Methods,” in *Handbook of Qualitative Research*, N. Denzin and Y. Lincoln (eds.), Second Edition, Thousand Oaks, CA: Sage Publications, pp. 769–802.

Samuelson, P. 2008. “EU Approach to Information Privacy Protection, Information Law and Policy” *University of California at Berkeley (Lectures)*, http://itunes.apple.com/de/podcast/eu-approach-to-information/id461118733?i=96857194, last accessed August 23, 2012.

Sitkin, S. B., and Roth, N. L. 1993. “Explaining the Limited Effectiveness of Legalistic Remedies for Trust/Distrust,” *Organization Science* (4), pp. 367-392.

Smith, H. J., Milberg, S. J., and Burke, S. J. 1996. “Information Privacy: Measuring Individuals’ Concerns About Organizational Practices”, *Management Information Systems Quarterly* (20:2), http://www.jstor.org/pss/249477, last accessed August 23, 2012, pp. 167-196.

Solove, D. J. 2002. “Conceptualizing Privacy,” *California Law Review* (90:4), http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1408&context=californialawreview, last accessed August 23, 2012, pp. 1088-1156.

Solove, D. J. 2006. “A Taxonomy of Privacy,” *University of Pennsylvania Law Review* (154:3), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622, last accessed August 23, 2012.

Spiekermann, S., Grossklags, J., and Berendt, B. 2001. “E-privacy in 2nd Generation E-Commerce,” *ACM Conference on Electronic Commerce (EC '01)*, Tampa, Florida: ACM Press, pp. 38-47.

APPENDIX A: CODES FOR PRIVACY CONCERNS

Machen Sie sich bei Ihrer Internet-/Facebook-Nutzung Sorgen über **Ihre Privatsphäre / den Schutz Ihrer Daten**? Wenn ja, **worüber machen Sie sich Sorgen**? Wenn nicht, **warum nicht**?

Category		**Subcategories - Content**	***Examples of Quotations***
Concerned because:			
Data Type	Bank data	Bank and credit card information	*Missbrauch von Kontodaten.* *Nur über alle Daten, die mit Online-Banking zu tun haben.* *Missbrauch von Bankdaten.*
	Online data	E-Mail account information, Login information, SNS user account information	*Mitlesen der Nachrichten.* *Dass Inhalte aus persönlichen Nachrichten entnommen werden. Passwort ist leicht zu knacken.* *Weitergabe von E-Mail-Adressen.*
	Personal data	Name, address, phone number, gender, birth date, photos	*Die anderweitige Nutzung von Fotos.* *Dass andere Nutzer sich Zugang zu meinen persönlichen Daten beschaffen.* *Fremde Nutzung meiner Fotos.* *Weitergabe und Speicherung meiner persönlichen Daten.* *Adresse, Telefonnummer und Name werden weitergegeben.*
Explicitly Mentioned Threats		**Subcategories - Content**	***Examples of Quotations***
Collection	Collection / Saving	Data storage and collection	*Bilder kann jeder abspeichern.* *Die speichern zu viel und zu lange*
Secondary Use	Analysis	Data aggregation, analysis and profiling	*Man erhält viel Werbung, die auf einen zugeschnitten scheint.* *Ausforschung meines Profils zu Datenzwecken.* *Dass Profile erstellt werden.* *Später werden womöglich Persönlichkeitsprofile erstellt.*
	Sale	Sale and trade of data	*Dass meine E-Mail-Adresse verkauft wird.* *Darüber, dass mit meinen Daten Handel betrieben wird.* *Verkauf von Daten.* *Verkauf von Adressen.*
	Identity Theft	Identity theft	*Identifikationsdiebstahl.* *Identitätsklau.* *Identity Theft.*
	Abuse / Misuse	General misuse	*Missbrauch von Daten.* *Missbrauch von Kontodaten*
Unauthorized Access	Dissemination	Dissemination and publishing of data	*Weitergabe meiner Daten.* *Datenweitergabe an Dritte.* *Meine Daten werden an Unternehmen weitergeleitet.* *Dass die Daten veröffentlicht werden.* *Weitergabe und Veröffentlichung der Daten.*
	Access	Access to data	*Sichtbarkeit von sensiblen Daten.* *Wer kann diese Daten alles einsehen.* *Dass persönliche Daten und/oder Fotos Dritten zugänglich gemacht werden.* *Zugang zu privaten Fotos/Posts.*
	Surveillance	Spying and tracking of data	*Ausspionierung.* *Ausspionieren von wichtigen Daten.* *Nachverfolgung von Behörden.*
	Stalking	Unauthorized access to data	*Ich kann gestalkt werden.*
Explicitly Mentioned Sources of Threats		**Subcategories - Content**	***Examples of Quotations***
(Future) Employer		N.A.	*Weil eventuell zukünftige Arbeitsgeber aufgrund von Fotos und Kommentaren falsch über mich urteilen könnten.* *Ob meine Außendarstellung oder meine Freunde den Leuten gefallen, die mich einstellen möchten.*
Marketing		Advertising Companies	*Nutzung meiner Daten für wirtschaftliche Zwecke/Werbung.* *Dass meine persönlichen Daten an zwielichtige Unternehmen verkauft werden könnten.* *Dass meine Daten gegen meinen Willen zu Werbezwecken genutzt werden.*
Hackers / Criminals		N.A.	*Datendiebstahl.*

		Datendiebe. *Darüber, dass v.a. kriminelle Organisationen/Hacker meine Daten (z.B. durch Trojaner) abfangen und missbrauchen.*
State / Government	N.A.	*Nachverfolgung von Behörden.* *Vermengung von privatrechtlichem Datenschutz/-sammlung in der Wirtschaft und staatlichen zentralisierten Datensammlungen der Repressionsorgane bis hin zur Privatisierung von rechtsstaatlichen Institutionen.*
Viruses	Malware	*Dass Viren oder Hacker auf den eigenen PC zugreifen.* *Passwortklau durch Viren.* *Trojaner.*
Facebook (as a Company)	N.A.	*Allerdings macht es mir Sorgen, dass FB gewisse Dinge nicht mehr rückgängig machen lässt. z.B. kann meine seine Infodaten im Bezug auf Interesse nicht mehr löschen.* *Ich finde es prinzipiell scheiße das auch gelöschte Dinge weiterhin von Facebook gespeichert werden.* *Facebook speichert alles auf Ewigkeit. Ich kann nicht entscheiden, dass meine Daten dauerhaft gelöscht werden.*
Friends from a Contact List		*Dass Informationen über Freundes-Freunde verteilt werden könnten.* *Wenn ich mir Sorgen mache, dann nur über Kommentare meiner Freunde, die meine Identität nachvollziehbar machen.*
Data Control	**Subcategories - Content**	***Examples of Quotations***
Longevity of Data	Unlimited data storage, long-term accessibility	*Alles kann nach Jahren noch eingesehen werden.* *Alles wird gespeichert, obwohl es für die User so aussieht, als wäre es gelöscht.* *Dass die Daten immer im Internet bestehen bleiben, auch wenn man diese löscht.* *Dass auch nach Jahren Informationen über mich im Internet zu finden sind.* *Die speichern zu viel und zu lange.*
Inability to delete data	Impossible to delete data	*Dass ich diese Daten nicht vollständig löschen kann*
Privacy settings not transparent	Difficult and unclear how to protect data	*Privatsphäre Daten/Sichtbarkeit kann jeder selbst festlegen für einzelne Personen. Liegt leider sehr versteckt.* *Angaben zur Kontoeinstellungen sind sehr kompliziert bis unverständlich geschrieben, so dass der Nutzer sich nicht länger damit beschäftigen will.* *Die Privatsphäreeinstellungen sind furchtbar verstrickt. man hat keinen guten Überblick darüber, wer was sehen kann.*
General loss of control over data	General feeling of helplessness and powerlessness with regard to use and protection of data	*Die Sorgen, die ich mir mache resultieren daraus, dass ich nicht weiß was genau mit meinen Daten passiert.* *Dass irgendwann meine Daten für andere Dinge, als die in den AGBS beschrieben, genutzt werden.* *Darüber, dass ich unwillentlich zu viel von mir preisgebe.* *Ich habe keine Kontrolle darüber, was mit diesen Daten passiert*
General loss of privacy	General fear of loss of privacy and unlimited data accessibility	*Die Gefahr, dass die Weitergabe vertraulicher Daten immer mehr Personen im Internet mehr und mehr gläsern werden.* *Gläserner Mensch.* *Verlust Privatsphäre.*
Unconcerned because:	**Subcategories - Content**	***Examples of Quotations***
Privacy Management Strategies		
Attitudes towards Privacy	"It won't happen to me!"; "I have nothing to hide"; "I don't mind publishing data"; "I don't care"	*Nichts zu verbergen.* *Weil die Infos, die ich über Facebook teile nicht sooo privat sind und das ruhig alle wissen können.* *Ich selbst habe nichts zu verbergen.* *Es ist mir egal.*
Self-Control	Little disclosure; disclosure of only "public" information; use of technical means; restrictive privacy settings	*Ich stelle nur Daten zur Verfügung, die mir öffentlich keine Probleme machen können.* *Ich stelle nur das online, was andere sehen sollen.* *Ich habe selbst entschieden, mich dort anzumelden und Daten preiszugeben.*

Anonymization	Use of pseudonyms	*Ich mache mir eigentlich kaum Sorgen, da ich weder mit meinem richtigen Namen noch mit irgendwelchen Fotos von mir dort vertreten bin.* *Ich bin nicht unter meinem richtigen Namen bei Facebook angemeldet damit nichts auf mich rückführbar ist (spätere Arbeitgeber etc).* *Fiktiver Benutzername.* *Den restlichen Teil des Internets nutze ich so anonym (Kosenamen….), dass ich mir dort relativ wenige Sorgen mache.*

APPENDIX B: CODES FOR LEGAL ASSURANCE

Glauben Sie, dass die in Deutschland bereits vorhandenen Gesetze **den Internet - / Facebook-Nutzern** einen wirksamen Datenschutz bieten? **Wenn ja, warum? Wenn nicht, warum nicht?**

Codes	**Subcategories - Content**	***Examples of Quotations***
Effective because:		
Law offers protection	I trust the law; Law offers at least some protection; Observed progress in protection; Privacy is often discussed in the media and by policy-makers; Observed progress in privacy policy-making;	*Der Internetbenutzer wird als schutzbedürftiges Wesen verstanden und als Verbraucher besonders geschützt. Die Ausnutzung von Schwächen im Selbstschutz der User wurden bereits Grenzen gesetzt.* *Auch wenn es sicherlich noch etwas zu verbessern gibt, bieten die vorhandenen Gesetze zumindest einen Grundschutz.* *Gesetze sind der Grundstein eines rechtsstaates und sie sind bindend* *Die wirkliche Gefahr der Internetkriminalität, d.h. Betrug, Diebstahl usw., wurde schon relativ stark erschwert.* *„Zudem sind die Datenschutzbeauftragten der Länder sehr aktiv. Aber diese könnten noch weiter gestärkt werden.“*
German law is strong	Laws in Germany is better than in other countries	*Die deutschen Datenschtzrichtlinien sind im internationalen Vergleich recht progressi.*
Self-responsibility of Users	Users are responsible for their own privacy; Users should control themselves It is not responsibility of the state	*Es ist doch wohl die eigene Sache, was man wie einstellt bei Facebook.* *Wer zu dumm ist zu verstehen, dass facebook offen für jedermann ist, der ist dafür doch eigenverantwortlich oder?* *Es liegt meistens an einem selber, dass man zuviel preisgibt.*
I had positive past experience	Lack of negative experience. Hence, derived conclusion about present protection.	*Weil ich bislang noch keine negativen Erfahrungen gemacht habe*
Ineffective because:	**Subcategories - Content**	***Examples of Quotations***
Facebook has power	Facebook has power; Facebook does what it wants.	*Facebook hat zu viel Macht und der Staat hat nicht genug Einfluss auf Facebook, um einen passenden Datenschutz durchzusetzen.* *Facebook macht, was es will.*
Laws do not cover everything	Perfect protection impossible; Laws not precise enough; Loopholes in the law; Law is cumbersome; Law is not flexible; AGB vs. Laws	*Es wird nie einen wirksamen Datenschutz geben. Erst recht nicht, wenn der Staat privatangelegenheiten sichern soll.* *Da es Schlupflöcher gibt die FB nutzt um den Datenscchutz in Deutschland zu umgehen;* *Wir brauchen keine Gesetze die mehr Datenschutz vorschrieben, wenn wir duch Bestätigen der Nutzungsbedingungen eh diese unwirksam machen.*
Law can be broken	Commonly broken; Abuse is always possible	*Betrug ist immmer möglich* *böswillige Hacker interessieren die Gesetze nicht. Und gefasst werden müssen sie auch erst noch.*
Law is hard to enforce	No efficient control mechanisms Inability to enforce; No resources to enforce	*böswillige Hacker interessieren die Gesetze nicht. Und gefasst werden müssen sie auch erst noch.* *das wichtige schein ja vor allem zu sein, dass es keine kontrolle gibt ob jemand mit dem datenschutz rechtmäßig umgeht.*
I distrust policy-makers	Lobbyism; Policy-makers are driven by industry; Policy-makers do not represent interests of users; Government itself abuses data; Distrust towards state; Policy-makers have no clue about Internet.	*Die Politiker haben keine Ahnung vom Internet und sind nicht in der Lage, Gesetze zu entwickeln, die der Dynamik des Internets gerecht wird;* *Facebook interessiert sich wenig für deutsche Gesetze. Der Staat ist der grösste Schnüffler, hat kein Interesse an wirksamen Gesetzen.*
I observe negative practices	Negative media coverage of privacy abuses; Observed Abuse; Observed Practices; Past Experience	*Daten werden weitergegeben veröffentlicht.* *Täglich Beispiele mit Fake Accounts, FB selbst missbraucht die Daten.* *Weil Facebook mit den daten machen kann, was es will. und dies auch tut.*
I do not know which laws exist	Lack of transparency; Lack of consumer information; Users do not know what is protected and what is not	*Erstens, weil ich sie nicht kenne;* *Es herrscht keine Klarheit darüber, was genau eigentlich Rechte der Nutzer sind und was mit den Daten gemacht wird.*
German law is local	Law is national, Internet is transnational; German law does not cover international companies	*...Außerdem werden deutsche Gesetze eine amerikanische Multi-Milliarden-Firma kaum kontrollieren oder einschränken können.* *...Weil ich glaube, dass facebook amerikanischem (oder irischem - auf*

	Laws not uniform enough across countries	*jeden fall nicht deutschem) recht unterliegt.*
Technology is always ahead	Technology always ahead of legal advances; Law is old; Law does not cover Internet / Social Media	*Es gibt allerdings noch enorm viel Nach-/Aufholbedarf, gerade im Bereich social Media.*

ABOUT THE AUTHORS

Dr. Hanna Krasnova is now a senior researcher and academic director of the Master Program in Information Systems at the Humboldt-Universität zu Berlin, Germany, where she received her Doctoral Degree. Hanna holds a Master of Science Degree in Banking and Finance from Belarus State University as well as a Master of Arts in Economics and Management Science from the Humboldt-Universität zu Berlin. In her research she addresses the issues of social, individual and enterprise value of the emerging Web 2.0 applications. She is the author of over 25 research articles published in the *Journal of Information Technology*, *Journal of Wirtschaftsinformatik*, *Identity in the Information Society Journal*, *International Conference on Information Systems* as well as other IS conferences. The paper she co-authored "*It's All About Networking! Empirical Investigation of Social Capital Formation on Social Network Sites*" has received the *second runner best paper award* at ICIS 2011 in Shanghai, China. Hanna has served as an associate editor at the Australasian Conference on Information Systems (ACIS) 2011 conference, the European Conference on Information Systems (ECIS) 2012 and will chair the track "*Social Media and Society*" at the upcoming ECIS 2013.

Paula Kift received a Bachelor's Degree with Highest Honors from Princeton University in the Department of French and Italian, with a focus on political science. She also pursued certificates in European Cultural Studies and Near Eastern Studies. As part of her undergraduate studies, she spent two semesters abroad, one at the University of Barcelona and one at the Sorbonne in Paris, where she worked as an intern for the Catalan Educational Ministry and the French Senate, respectively. Paula spent a summer conducting research on the Ottoman Empire at the Center for Anatolian Civilizations in Istanbul, Turkey, and dedicated two weeks of her undergraduate program to studying human rights, politics and religion in Venezuela and Bolivia as part of a human rights delegation organized by *Witness for Peace*. She is currently employed as a research assistant at the Humboldt Institute for Internet and Society, where her primary interests reside in European legislation of data protection and the use of Internet for political participation. In September, Paula will begin a Master of Public Policy at the Hertie School of Governance in Berlin.