TOWARDS A TAXONOMY OF PERCEIVED CONSEQUENCES OF PRIVACY-INVASIVE PRACTICES

Complete Research

Hauff, Sabrina, University of Augsburg, Augsburg, Germany, sabrina.hauff@wiwi.uni-augsburg.de

Veit, Daniel, University of Augsburg, Augsburg, Germany, veit@wiwi.uni-augsburg.de

Tuunainen, Virpi Kristiina, Aalto University, Helsinki, Finland, virpi.tuunainen@aalto.fi

Abstract

Internet users are increasingly concerned about their information privacy based on how individuals and organisations access and handle personal information. So far, literature has mostly dealt with information privacy concerns, referring to how individuals perceive organisational privacy practices, or with privacy risks in general. Yet, a deeper understanding is missing regarding the consequences individuals perceive to arise from privacy-invasive practices, i.e. the negative outcomes that people are afraid of due to an infringement of their privacy. To fill this gap in research, we systematically investigate how perceived privacy-invasive data collection and usage can affect individuals. Based on our focus group data, we develop a taxonomy of perceived consequences of privacy-invasive practices. It consists of six identified categories of consequences, namely social, psychological, resource-related, independence-related, legal, and physical consequences, and several privacy-specific subtypes within these categories.

Keywords: Information Privacy, Perceived Consequences of Privacy-invasive Practices, Privacy Risks, Focus Groups.

1 Introduction

People in today's society spend a lot of time with online activities like searching information on the internet, shopping online, and interacting with friends in social networks. On the one hand, the internet enables comfortable searching and sharing of information and thus has become an integral part of both our private and professional lives. On the other hand, all internet users leave numerous data traces that contain personal information and reveal details about their behaviour, preferences, and personality. In addition to that, most people can be easily identified online, either when they provide required information on a voluntary basis, for example in online profiles of social network sites (SNS) or e-commerce platforms; when they allow cookies to be installed on their computers; or in more unaware manner through the combination of several other technical parameters, for example, the operating system, the colour depth of their screens, or their Domain Name System profiles (Takeda, 2012). Remarkable price erosion for data storage over the last decades combined with technological advances in the area of data mining allow the collection, storage, and analysis of large amounts of personal information (McAfee and Brynjolfsson, 2012). Companies like Facebook, Google, or Amazon are heavily using the so gained knowledge to personalize their service offerings. This way they can better address customer interests and increase their profits.

Internet users are getting increasingly aware of these practices and many surveys constantly show the high concerns people voice regarding their privacy in the internet (BCG, 2013; TRUSTe, 2013).

Extant research on information privacy has paid a lot of attention to information privacy concerns, which are used as central constructs in comprehensive literature reviews (Li, 2011; Smith et al., 2011). Information privacy concerns have been defined as the extent to which an individual is concerned about organisational practices of handling personal information (Smith et al, 1996). Many studies have found that information privacy concerns influence users' willingness to disclose personal information (Smith et al., 2011). Yet, other studies have shown that while people express serious concerns, they still often disclose significant amount of their personal information on the internet (Acquisti and Grossklags, 2005; Jensen et al., 2005; Norberg et al., 2007).

In this paper, we argue that we need a better understanding of what people perceive the impact of privacy-invasive practices to be. This is a necessary basis for gaining deeper insight into the relationship between perceptions of privacy, perceptions of consequences of privacy invasions, and actual behaviour. The concepts of information privacy concerns and privacy-protective responses are well defined in extant literature. Information privacy concerns examine people's perceptions on how organisations handle personal information, that is, whether they collect, analyse, use, and forward people's personal information, constituting potential privacy-invasive practices. Privacy-invasive practices describe the ways personal information might be handled by organisations or by other third parties so that a person's privacy is infringed. Son and Kim (2008) identified several privacy-protective responses that people might use when their privacy was invaded, including refusal of information provision, misrepresentation of information, or spread of negative word-of-mouth about the organisation. However, Dinev (2014) argues that people might have a limited knowledge and understanding of these privacy-invasive practices and how they impact individuals; in other words, what consequences can arise for individuals out of these privacy-invasive practices. Drawing on this, we think it is important to develop a systematic understanding of how privacy-invasive practices by individuals or organisations impact people. This is needed to better understand privacy-related behaviour: both information privacy concerns regarding organizational data handling and the consequences they perceive for themselves might shape people's behavioural reactions.

One concept used in literature is privacy risk. Risks in general can be described as a function of adverse consequences and uncertainty (Bauer, 1960). More specifically, privacy risks refer to the expected privacy loss and are defined as the "perceived risk of opportunistic behavior related to the disclosure of personal information submitted by Internet users in general" (Dinev and Hart, 2006, p.64). However, earlier privacy research describes privacy risks as one-dimensional and they are often investigated merely as the loss of control or the overall perceived risk (Malhotra et al., 2004; Dinev and Hart, 2006; Smith et al., 2011). In other contexts, risk has been found to consist of several categories, including for example social, psychological, or financial categories (Dowling, 1986). These can also be seen to apply to the context of privacy. For instance, due to privacy invasions, people could lose money if their credit card data is misused. This is a financial risk. Also, people might be concerned about a constant surveillance of their behaviour on the internet and a potential loss of their peace of mind. This is a psychological risk. Therefore, our aim is to investigate privacy risks in detail and identify their categories. More specifically, our focus is on one risk component, namely the adverse consequences. While consequences describe the form of a loss from privacy invasion, the second risk component, uncertainty, describes the probability of a consequence's occurrence. Therefore, it is subjective and situational by nature and not identifiable in general (Dowling, 1986). Even more, we have to get a clear understanding of the consequences first before we can investigate their likelihood. The overall idea of investigating privacy risks is also supported by Preibusch (2013) who calls for the development of new concepts in addition to information privacy concerns to enhance our understanding of the antecedents of online behaviour.

Based on the above discussion and argumentation, we see the investigation of perceived consequences of privacy-invasive practices highly relevant and increasingly important. Thus, we pose the following research question:

What are the perceived consequences of privacy-invasive practices?

With this research question, we look into how people perceive potential privacy invasions by both known and unknown individuals and organisations (commercial and non-commercial). We will introduce a taxonomy of perceived consequences of privacy-invasive behaviour in the internet, thereby not limiting our study to one context but incorporating all types of perceived consequences that are of relevance in the internet. This helps to advance both theoretical and practical understanding of how internet users' privacy perceptions influence their behaviour.

The remainder of this paper is structured as follows: In the next chapter, we give an overview on information privacy concerns and privacy risks and thereby build the foundation for our study. In the third chapter, we describe our methodology. We used focus groups to gather detailed insights into perceived consequences of privacy-invasive behaviour. We then discuss our findings and finish by highlighting theoretical and practical contributions of our research as well as directions for future research.

2 Earlier research

While there are several definitions of information privacy, they all have one thing in common, namely that they typically "include some form of control over the potential secondary uses of one's personal information" (Bélanger and Crossler, 2011). We adopt the well-established definition of Westin (1967) who also includes the control element by referring to information privacy as the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (p.7). In the following, we discuss the concepts of information privacy concerns and privacy risks as they are used in privacy research. We also discuss their limitations in explaining the adverse consequences of privacy-invasive practices for people.

2.1 Information privacy concerns

Information privacy concerns refer to the worries or anxieties that people associate with a potential loss of privacy (Bansal et al., 2010). They are used as proxy for information privacy and have evolved as the central construct in privacy research over the last years (Smith et al., 2011; Li, 2011). Especially the conceptualisations of Smith et al. (1996) and Malhotra et al. (2004) have received considerable attention and have served as basis for many studies.

Smith et al. (1996) conducted the first methodologically rigorous approach to analyse information privacy concerns and argue that they are multi-dimensional. They call the according instrument "Concern For Information Privacy (CFIP)". Information privacy concerns have traditionally been investigated as being one-dimensional, but often varied from study to study and without a common underlying framework (Smith et al., 1996). Smith et al. (1996) identified four central categories of information privacy concerns:

- collection, referring to the "concern that extensive amounts of personally identifiable data are being collected and stored in databases" (p.172);
- internal or external unauthorized secondary usage, describing the "concern that information is collected from individuals for one purpose but is used for another, secondary purpose, (eventually even) after disclosure to an external party" (p.172);
- improper access, being defined as the "concern that data about individuals are readily available to people not properly authorized to view or work with this data" (p.172), and
- errors, comprising the "concern that protections against deliberate and accidental errors in personal data are inadequate" (p.172).

The taxonomy categorises individuals' concerns about organisational information privacy practices (Smith et al., 1996) and has mostly been applied in offline or traditional direct marketing settings (Malhotra et al., 2004). While it focuses on how individuals perceive organisational behaviour

regarding the handling of personal information, it ignores the impacts of these perceived organisational information handling practices on individuals.

Malhotra et al. (2004) build on the work of Smith et al. (1996) and extend it to an online setting. Drawing from social contract theory, they define information privacy concerns as "an individual's subjective views of fairness within the context of information privacy" (p.337) and identify three categories, namely collection, control, and awareness. Their instrument "Internet Users' Information Privacy Concerns (IUIPC)" is conceptualized as "the degree to which an Internet user is concerned about online marketers' collection of personal information, the user's control over the collected information, and the user's awareness of how the collected information is used" (p.338). Similar to CFIP, IUIPC does not pay attention to the impacts of organisational behaviour on individuals, even though the category of control could be interpreted this way. Overall, IUIPC was also developed for e-commerce settings.

In contexts other than e-commerce, information privacy concerns are understood and used similarly. Hong and Thongh (2013) found users to have lower concerns regarding disclosure of information to governmental websites than to commercial websites. Yet, the expectations of how their data should be handled were the same in both settings. The same is true for privacy studies in the context of social networking. For instance, Chen et al. (2009) investigated information privacy concerns related to what peers disclose about friends: They looked into the practices of unauthorized use, improper access, and error. Neither of these studies on information privacy concerns considers how an individual might be impacted by privacy-invasive practices of other individuals or organisations.

2.2 Privacy risks

The concept of risk has its root in psychology research and has received much attention in consumer behaviour research. Risk is most commonly defined as comprising the severity of negative consequences of a situation and their probability of occurrence. However, the probabilities might be unknown and just refer to a good or bad feeling that influences the perceived subjective risk a person assigns to a potential outcome of a situation (Cunningham, 1967; Jacoby and Kaplan, 1972; Dowling, 1986; Mitchell, 1999).

The categories of risk have been widely debated. Earlier research has identified various types of losses, even though little consensus has been reached regarding their precise nature. Studies have used different categories depending on the context and the object under investigation. Yet, most often the following categories have been of interest and have been incorporated in research (Dowling, 1986):

- Performance risk which refers to whether the outcome is of the expected quality.
- Social risk which refers to whether the outcome leads to an individual's embarrassment in one's social group.
- Physical risk which refers to whether the outcome influences the individual's safety.
- Financial risk which refers to whether there is a monetary outlay associated with the outcome.
- Psychological risk which refers to whether an individual's peace of mind is affected.

The risk concept comprising these different types has proved useful for example in consumer behaviour research (Featherman and Pavlou, 2003; Luo et al., 2010a). In privacy research, however, the concept of risk has been treated in an inadequate manner. Privacy risks are often used as part of the privacy calculus perspective that assumes that a trade-off between risks and benefits determines users' behaviour. In this perspective, privacy risks have so far been assumed to be one-dimensional (Malhotra et al., 2004; Dinev and Hart, 2006; Smith et al., 2011). Dinev and Hart (2006) identified that these risks arise from different types of organisational actions, such as, unauthorized access and disclosure of personal information or improper access by hackers, third parties, or governmental

agencies. However, again the impact of privacy-invasive practices on the individual is not taken into detailed consideration. Smith et al. (1996) state that an individual's calculation of risks "involves an assessment of the likelihood of negative consequences as well as the perceived severity of those consequences (and that the) negative perceptions related to risk may affect an individual emotionally, materially, and physically" (p.1001). Yet, to our best knowledge none of the existing privacy risk conceptualisations follow this line of thought rigorously, nor do they investigate different categories of privacy risks.

3 Methodology

In the empirical context of our study, we conducted focus group interviews as our qualitative data collection method to better understand the types of individually perceived consequences of privacy-invasive practices. We invited several participants to discuss a specific topic of interest to the researchers and to provide their insights into their attitudes, perceptions, and opinions (Bélanger, 2012). In our case, focus groups were a suitable methodology as they allowed us to explore how privacy-invasive practices affect individuals. The focus group discussions entailed rich interaction among the participants, as they had to explain their opinions and provide good argumentation.

Based on Fern's (2001) classification of focus group method types, we chose the exploratory type. The purpose of exploratory focus groups is to identify, collect, and explain feelings, thoughts, and behaviour. It aims at uncovering everyday knowledge and at making it explicit to generate theoretical constructs, causal relationships, and theories. In comparison, experiential focus groups can be used to triangulate and confirm hypotheses and theories while clinical focus groups are used to explain feelings and behaviour that are suppressed or unknown to individuals but influence their preferences (Fern, 2001).

The decision to collect empirical evidence with exploratory focus groups guided the design and conduct of our focus groups. We followed the guidelines provided by Fern (2001) and used heterogeneous participants with respect to their privacy attitudes and knowledge about privacy-invasive practices for uncovering not only shared but also unique ideas. However, within each focus group, we chose homogeneous individuals with respect to their social environment and age. Due to the sensitivity of the topic, we expected individuals to disclose their feelings and perceptions more openly in a familiar environment. We also relied on Fern's (2001) guidance on the duration of sessions and number of participants. The latter one follows the same logic as with other qualitative methods: once saturation is reached and no new concepts and ideas emerge, one should stop gathering further data.

Altogether, we conducted seven focus groups: three with pupils, three with students, and one with adults, thereby putting the focus on younger subjects. Those individuals are digital natives who have intertwined the use of digital technologies with their daily lives (Vodanovich et al., 2010). They are especially suitable for identifying perceived consequences as they are constantly exposed to various online activities. Yet, our focus groups also showed that they critically reflect on privacy issues. Moreover, the focus groups with adults did not reveal any additional consequences compared to the focus groups with students and pupils. Table 1 gives an overview of all focus groups conducted. Each focus group was recoded and transcribed. The focus group moderator used a semi-structured interview guideline to start the discussion but then was very open to different directions the discussions could take and flexibly adapted the moderation to explore new and unexpected ideas. In particular, the participants were asked about activities they (do not) perform regularly in the internet and which information they (do not) share. Then, all activities in which personal information is knowingly or unknowingly shared were investigated in detail. This improved our understanding of the participants' behaviour, their concerns regarding privacy-invasive practices, and whether they perceived any impact of those practices. Moreover, the groups also discussed which information is sensitive and how to manage their privacy.

Focus group	Description	Number of participants	Age range	Duration
F1	Students of a German university (bachelor and master program)	5	21 to 25	1 hour 40 minutes
F2	Students of a German university (bachelor and master program)	5	22 to 24	1 hour 40 minutes
F3	Students of a German university (bachelor and master program)	4	22 to 24	1 hour 40 minutes
F4	Pupils of 11th grade of a German high school	8	17 to 18	1 hour 30 minutes
F5	Group of German adults	5	24 to 43	45 minutes
F6	Pupils of 8th grade of a German high school	6	13 to 14	40 minutes
F7	Pupils of 10th grade of a German high school	10	15 to 16	1 hour 15 minutes

Table 1. Focus groups

For data analysis, we coded the data using Atlas.ti[1]. We started with coding low-level concepts and phenomena and then build categories by putting together similar related concepts. Based on constant comparison of the data "to see if [the focus groups] support and continue to support the emerging categories" (Holton, 2007, p.277), we identified categories of perceived consequences of privacy-invasive practices and were able to summarize those concepts into higher level categories of consequences. Thus, our approach used the focus group participants' experiences with information privacy to develop a second-order theoretical understanding of perceived consequences of privacy-invasive practices (Lee, 1991; Sarker et al., 2012). Our approach can be described as a less procedural version of the grounded theory methodology as proposed by Sarker and Sarker (2009).

4 Results

In the following, we present our results and interpretations of individuals' perceived consequences of privacy-invasive practices. We start with a short summary of privacy-invasive practices. We then investigate in detail how these practices can impact individuals and develop a taxonomy that summarizes our findings.

4.1 Privacy-invasive practices

In order to understand which consequences individuals see as a result of privacy-invasive practices, it is first of all important to understand how one's privacy can be invaded. As explained in chapter 2, Smith et al. (1996) discuss four categories of organisational practices that could give rise to information privacy concerns. Those categories are collection, unauthorized usage, improper access, and errors. Our focus group participants named all of those practices as well, even though they did not only relate them to a commercial organisational context, but also elaborated on how individuals and governmental agencies might invade their privacy. The same categories apply.

To give an example regarding **collection**, one participant said:

"I think the biggest problem is if you own an Android smartphone and also use other Google services, then Google has an almost complete life story of you. It has complete location information of your whole life since you own an Android smartphone, a complete search history, not only based on your IP but eventually under your name, if you have a Google-account. (…) They know everything about you." (participant in F3)

[1] We used Atlas.ti version 7.5.2 for coding our data.

In this case, it is not just the information one knowingly shares with an organisation, but he also hints at the unconscious constant data collection that happens.

Regarding **errors**, one participant told that she was afraid of other individuals spreading wrong information about her:

"For me, sensitive data would also comprise that someone starts a rumour about me. I would be really mad, especially if it is wrong, if it is just not true, and I'll find it out or it is has been posted via a social media platform and thus can hardly be removed."(participant in F2)

Improper access has often been named with respect to organisations that display advertisements based on individuals' search history they took from other sources or with respect to individual hackers that are interested in account and credit card information:

"Lately, I've searched for a cap via Google. I just googled it and picked one I liked and saved it in my favourites. Then I went to Facebook and the exactly same cap was offered to me at the side banner."(participant in F4)

"I'm more afraid of hackers or other single persons who might be interested in students and could do a lot of harm. (…) I don't think that Google would sell my account information. I'm not afraid of that. I'm more afraid of hackers who might get access to my data and misuse them for something I dislike." (participant in F1)

Lastly, **unauthorized secondary usage** of information has again often been mentioned in an organisational context, for example for marketing purposes, but also in private settings. One participant told that she often went to parties with friends and then the following happened:

"A friend of mine and me, we made strange pictures and it was really funny, we had a lot of fun. Yet no one has to know of that. But she uploaded one of those pictures as her cover photo. I found that really terrible and it took me a lot of time to convince her to undo that (…). The bad thing is that if something like this happens, it'll never be forgotten, as I said in the beginning."(participant in F4)

To sum up, all different categories that we already know from literature have also been identified by our focus group participants. Even more, we found support that those practices can also be executed not only by organisations but also by individuals. We can now build on those practices to investigate the related perceived consequences and the effect they have on individuals.

4.2 Perceived consequences of privacy-invasive practices

Based on our focus groups, we identified six categories of consequences, namely social, independence-related, resource-related, legal, psychological, and physical consequences. They depict different ways of how individuals can be impacted by privacy-invasive practices. More specifically, they describe how individuals can perceive to be negatively affected by practices such as collection, the unauthorized usage, the improper access, and errors of personal information. Those practices per se do not have to harm individuals. However, negative outcomes might arise from those practices which we refer to as consequences of privacy-invasive practices. We develop a taxonomy that summarizes those results. The taxonomy is summarized in Figure 1 in chapter 4.3 and the categories are introduced in detail in the following.

4.2.1 Social consequences

Social consequences comprise all fears about a change in social status as a result of privacy-invasive practices. Three different types of social consequences can be differentiated. First, others might do a prejudged evaluation of an individual based on the information that someone gathered online. This could be an impression one gets from the information available in SNS, for example from status messages, pictures, profile information, or likes with which someone expresses that he or she is fond of something or someone. Another source of information is publicly available information that can be found via search engines. As a consequence of access to this information, others develop an idea of the opinions and the behaviour of an individual. If individuals dislike this pigeonhole thinking and are

worried about the impression that others now have of them, then an individual is bothered by a **prejudged evaluation**:

"I've lately googled myself. The first hit I got was a comment about American beer I made in some forum during the time of the soccer world cup in 2006. I said that it tastes like piss (at a time I was 15 and thus not even officially allowed to drink alcohol). When I saw that I thought 'seriously'? (…) This shouldn't be the first hit someone gets about me on the internet." And further on he said: "*When I think back how I behaved five years ago, I don't want others to see that now. I want to freely develop myself, without being put into a stereotype for the next years." (participant in F1)*

A related idea was raised by another participant:

"The problem with pictures is that you only see a detail of a scene, but you don't know what happened before or after and in consequence, you sometimes appear in a bad light." (participant in F7)

Second, a **loss of respectability** is a further social consequence. It occurs if in addition to a negatively perceived image others subjectively condemn certain behaviour, independent of whether it is actually questionable:

"Another problem is that one could lose respectability. (…) When I google teachers of mine or enter them into Facebook, then you'll get pictures. For one teacher, I got the information that she got an eye treatment by laser surgery (…) in Istanbul, and I think this is so highly dubious, so that I thought "oh ok". And for another teacher, you'll get some strange pictures. Once you've seen them, you cannot look at him without thinking "ah, ok"." (participant in F7)

Third, **calumny and mobbing** describe another subcategory of social consequences that individuals can be afraid of. Based on opinions, pictures, or other available information, people could be harassed:

"*Via Whatsapp, I only send pictures to people who I really trust, especially the ugly ones. I know, when I post them into this group, they won't be passed on to others. What happens in this group stays in this group, to say it. On Facebook, there is the danger of cyber mobbing and stupid comments, I just want to avoid that. I don't want to be exposed to that." (participant in F7)*

In addition, people might also fear that others spread misinformation to harm someone:

"*For me, sensitive data would also comprise if someone starts a rumour about me. I would be really mad, especially if it is wrong, it's just not true, and I'll find it out or it is has been posted via a social media platform and thus can hardly be removed." (participant in F2)*

4.2.2 Independence-related consequences

Independence-related consequences refer to the fear of manipulation as a result of privacy-invasive practices. In particular, they present one way of how personal information can be abused. Individuals might perceive that they no longer have a free choice of how to behave and what to believe in because they might only be confronted with predetermined and selected pieces of information, not the whole unfiltered flow of information. Two different types of manipulation could occur. Individuals can fear that either their behaviour or their opinion is aim of the manipulation. Based on personal information that organisations collect and analyse, they get a good idea about people's habits, preferences, and opinions. However, if organisations have knowledge on these aspects, they might try to **manipulate a person's behaviour**. Personalized advertisements are one form of manipulation intentions:

"Everyone knows that you get personalized advertisements in the internet, e.g. based on what you just looked at. But how much can they manipulate with these data? How much do we realize? We'll never know how much it influences us. Would I have bought a certain product anyway or have I bought it only due to the manipulation?" (participant in F7)

Regarding a **manipulation of a person's opinion**, a perceived consequence deals with governmental agencies that might be interested in censoring information:

"If I submit a Google search query, then they save my whole history. If they then want to manipulate which information I can see about current topics, then it'll be possible to heavily censor that. Thus, we

again address the topic of governments. If somehow a government might either put pressure on Google or offers incentives to Google to censor something or to manipulate the opinions of certain people, then I perceive that as really dangerous." (participant in F3)

4.2.3 Resource-related consequences

We define resource-related consequences as the fear of a loss of resources due to privacy-invasive practices. Two types of resource-related consequences can be differentiated: financial and time-related losses. **Financial losses** are especially associated with an improper access of account information, for example by third parties that hack into an account:

"Regarding online shopping, my biggest concern is that my account information is stolen and that huge amounts of money are debited. (…) The risk is there. This is always in the back of my mind." (participant in F3)

A **loss of time** has also been identified as consequence. For example, e-mail addresses are misused and spam mails are constantly sent that an individual has to deal with. Another interesting example was given by a student. She described that she disclosed her cell phone number in a lottery and now constantly gets called by various unknown numbers:

"On the internet, it is said that this are rip-off artists who want to sell some holiday offers. If I don't answer them, nothing will happen to me. However, they probably want to get more data about me, I don't know. I always block their numbers, when they are using a new one. Then, I google it to check who that could be, and it always says that this aren't reputable callers." (participant in F3)

Moreover, she told that she already tried to find out who was responsible for the lottery and went through all her e-mails without any result. Overall, she is investing a lot of time to solve this hassle.

4.2.4 Legal consequences

Legal consequences refer to the **fear of being made responsible for actions someone did in another person's name** and thus misused the person's identity. Individuals are then worried that the identity is used to commit fraud or other crimes and that they might be held liable for that. A student told that her e-mail account got hacked and she was worried about the following:

"But my biggest concerns were that someone commits with my e-mail address, in my name, fraud. That he sends offers to others that I'm hold liable for." (participant in F3)

4.2.5 Psychological consequences

Psychological consequences comprise all types of fear that an individual's peace of mind is negatively affected as a result of privacy-invasive practices. It means that those practices are constantly present in an individual's mind so that the individual perpetually thinks about it and thus is under constant psychological pressure. We identify four types of psychological consequences. First, individuals can have a **constant feeling of surveillance**. They are afraid that every single action they do in the internet is monitored and analysed which puts a major burden on them and an uneasy feeling. For example, one focus group discussed about Anonymous, a loosely associated international network of activist and hacktivist entities:

"Yes those guys with the masks. I like what they do and it's important. But I didn't dare to like them on Facebook, even though I'd love to get their news in my newsfeed. I mean, I don't know who might get to know about that and how that could fall back negatively on me. I don't know whether this is an unjustified fear, but it is strange and I behave totally different, only due to this constant feeling of surveillance." (participant in F4)

Moreover, friends and acquaintances can also be a source of surveillance fears:

"What happened often to me is that my sister and my friends tagged me everywhere. Well, I didn't like that. (…) It is an unwell feeling when other people know where you are."(participant in F5)

Second, individuals can perceive a **pressure of constant mindfulness and attentiveness** as to which information they share. They have the impression that they constantly have to evaluate and critically analyse their online behaviour in order to identify all potential harmful consequences of this behaviour that could occur in the future:

"I often think about the following issue: In your youth, everyone makes mistakes and those mistakes might of course be also visible via Facebook or via the internet in general. If our parents made something stupid, then it was forgotten five years later. For us, it is theoretically, or not only theoretically, the possibility really exists, that it'll again surface in 40 years, once a stupid picture got published, whether you wanted that or not and whether you thought about it thoroughly or not. This is really frightening and restricts my freedom of what I'd like to do. Every time, I have to fully evaluate how to present myself and what I do online. It's a pity because in your youth, you should have fun and so on, but that is how it is." (participant in F4)

Another psychological consequence is a **feeling of a loss of control**. Once information has been shared, individuals might perceive that they can no longer decide on who has access to their information and how their information is used. The loss of control can bother people so that it is constantly in their mind. It leads to stress and a mental burden due to the perceived helplessness and powerlessness:

"Just recently the issue emerged that all pictures which we upload and everything that we write could be used for advertisements and similar things. I was really scared when I heard of the possibility that my profile picture could be displayed on a poster two days later somewhere in the city." (participant in F4)

It can also be a perceived loss of control, where control could be gained back with high effort:

"What really bothered me is that Facebook-Apps just make things public without asking whether that is alright for the user. Perhaps it's written down in small print which I usually don't check. For example, I pledged for an orchestral work on Kickstarter, so that it can be performed, and I would get the recording. The work was called "Totmorden", which is a rather polarizing term for Germans and which you do not want to be associated with your name if a potential employer is checking you out on the web. (...) And if you googled my name, you could see that I pledged for their project, which I didn't find cool." (participant in F3)

Lastly, individuals can also have a general **feeling of uncertainty** as a diffuse, abstract threat. They currently do not see any specific consequences. Yet they are afraid that at some point in time there could be negative consequences and this issue already impacts their peace of mind:

"An extreme example: I've googled the basics of Scientology or (Hitler's) "Mein Kampf" because I was interested in it. I also read several other books, but you wouldn't want this to appear alone, that you read something like that. Just because you might be interested in it from a historical perspective. It's really totally harmless. If you take all books that you've read at some point in time and in which you are interested, then you'll get an innocent impression of me. (...) There is a feeling of unease, even though it doesn't make any sense, as they already know everything about you. So this fear is not really rational, but I have this bad feeling when I do certain things on the internet." (participant in F3)

4.2.6 Physical consequences

Physical consequences refer to the fear of a **loss of physical safety** as result of privacy-invasive practices. If personal information is easily available online, it can be used to find out where a person stays. For example, if a person had an argument with someone or if others want to punish a person, e.g. for certain behaviour or an opinion, the availability of location information can lead to physical violence against that person:

"Once I was threatened by someone via Facebook. I was really extremely glad that I hadn't published any sensitive data online. I was really scared because if my city and my real name had been available, it wouldn't have been too difficult to identify and find me in a city not too big." (participant in F2)

4.3 Taxonomy of perceived consequences of privacy-invasive practices

Figure 1 summarizes our results and graphically depicts our preliminary taxonomy. We developed this taxonomy based on the data from our focus groups. It consists of the six categories physical, social, independence-related, resource-related, legal, and psychological consequences as well as several subcategories.

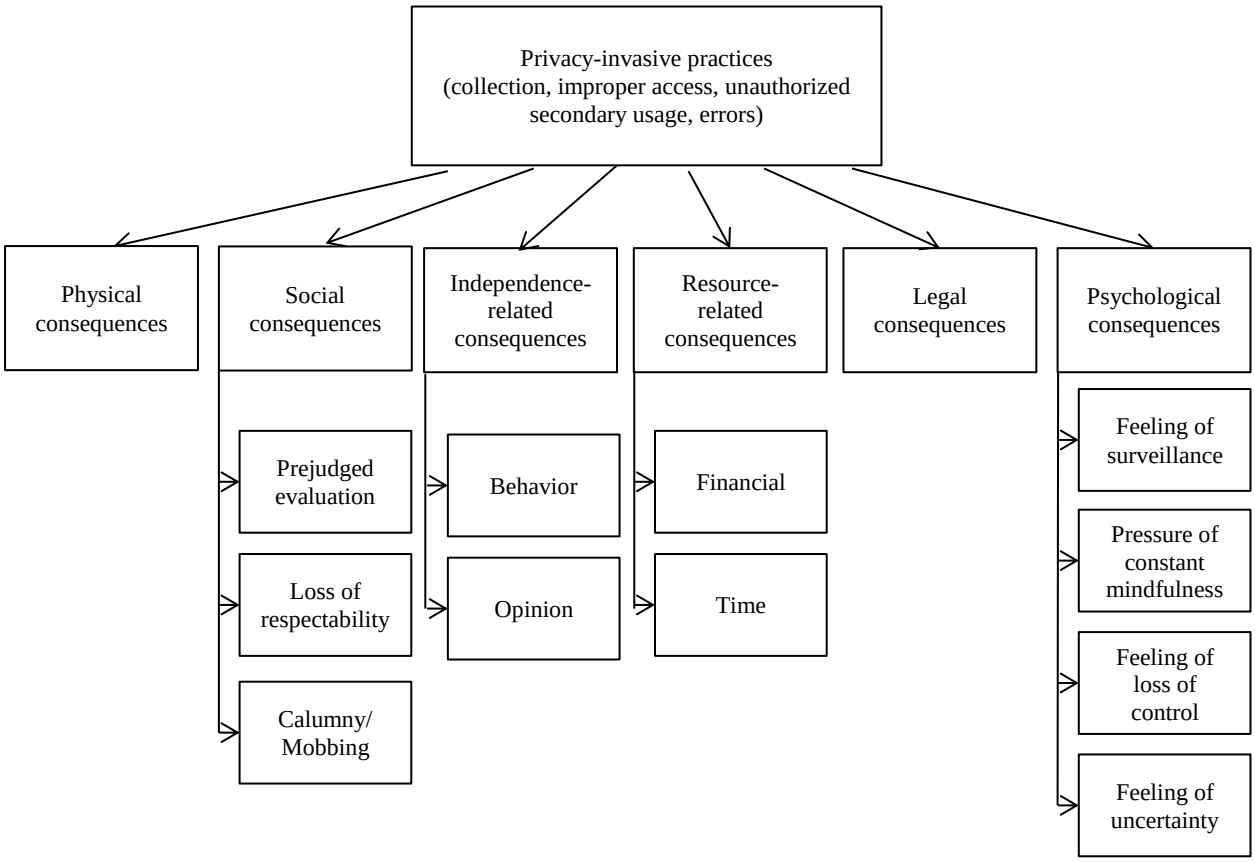

Figure 1. Taxonomy of perceived consequences of privacy-invasive practices

Our taxonomy is a first approach towards categorizing perceived consequences of privacy-invasive practices. We believe this taxonomy helps to better understand how privacy-invasive practices and the way individuals perceive them affect individuals.

5 Discussion

The main purpose of this study was to advance theoretical understanding of information privacy. We developed a taxonomy of perceived consequences of privacy-invasive practices and classified the impact individuals expect due to these practices into six categories. In addition to recognizing that these practices affect individuals it is important to understand what different types of consequences individuals can perceive.

Our results have several theoretical implications. So far, privacy research has focused on information privacy concerns, meaning how individuals perceive organisations to handle their data, and on privacy risks in terms of the expected loss of privacy. However, privacy risk has been conceptualized as a single-dimensional construct, focusing on the overall risk perception. None of the earlier studies have fully captured how individuals perceive the ways an invasion of their privacy could harm them. By

investigating how privacy-invasive practices affect individuals, we aimed at filling this gap. The focus of our investigation was on one component of risk: the adverse consequences. These adverse consequences have to be understood before the second risk component - a subjective likelihood of the consequence's occurrence – can be evaluated. We offer insights into the consequences individuals might perceive to occur when their privacy is invaded by other individuals or organisations. We found six categories of consequences, namely social, psychological, resource-related, independence-related, physical, and legal consequences. Even though four of the identified high-level categories are in line with earlier literature, our taxonomy introduces novel privacy-specific forms of those consequences. They are different from risk categories in other areas, such as e-commerce. For instance, psychological risks in earlier literature have been referred to as the risks "that the service will lower the consumer's self image" (Luo et al., 2010, p.226). However, this type of risk does not seem to play a major role in privacy. We found evidence for other forms of psychological consequences in privacy, namely the mental stress that people experience when having to decide whether or not to disclose certain information because there could be negative consequences associated with this decision. Another form is the constant feeling of surveillance that is also very specific for privacy. Thus, although the overall categories of consequences are similar on an aggregated level, the particular instantiations can vary widely for several categories. Moreover, we found two categories, namely legal and independence-related consequences, which are specific to a privacy context.

Our taxonomy can also be used as a helpful classification tool when only specific consequences are taken into consideration. Since the earlier conceptualisations of information privacy concerns and privacy risks offer only limited explanation of online user information disclosure behaviour, we believe that the viewpoint of perceived consequences of privacy-invasive practices can be an interesting new perspective on this topic.

Our results also offer implications for practice. Our insights into how privacy-invasive practices can impact online users can help organisations to analyse which of these consequences arise from their practices and how they can be influenced and possibly also mitigated. In addition, some consequences might be linked to certain parties, for example social consequences mostly arise from privacy-invasive behaviour of individuals or psychological consequences such as a constant feeling of surveillance can be traced to governmental agencies. Recognizing and mitigating these consequences is the responsibility of relevant authorities.

6 Conclusion and outlook

Many studies in privacy research have focused on information privacy concerns. While it is important to understand how individuals perceive organisational privacy-invasive practices, so far research has neglected how these practices can impact individuals. Yet, without a systematic and holistic understanding of these perceived consequences it is difficult to understand how individuals are affected by privacy-invasive practices. Our taxonomy of perceived consequences of privacy-invasive practices sheds light on these issues by categorizing the consequences that can be perceived to affect individuals if their privacy is invaded.

Nevertheless, more research on this area is clearly needed. We see several directions for future research on privacy: First, it would be useful to understand in more detail the types of perceived consequences in different contexts - for example SNS, e-commerce and information search - and the sources of the different consequences. It would also be interesting to better understand which factors influence the perceived consequences of privacy-invasive practices and whether and how they can be mitigated.

Moreover, our taxonomy can serve as basis for the development of new scales of measurement for empirical studies on privacy risk as multi-dimensional construct. As the impact of those practices on individuals has not yet been investigated in privacy research, it is necessary to develop new research

instruments. However, since other areas like consumer behaviour research have already investigated risk as multi-dimensional concept, it might be helpful to build on those scales wherever possible.

Finally, a promising avenue for future research would be to test whether and how perceived consequences of privacy-invasive practices influence actual online user behaviour. Our focus group participants mentioned that they behave differently if the consequences are severe and likely to occur. Yet, there might be a certain threshold that has to be reached before behavioural changes can be noticed. This is also of interest to practice. Many business models like those of SNS providers or e-commerce platforms depend on the collection and analysis of user data. It is of crucial importance for these organizations to understand online users' information privacy concerns and consequent information disclosure behaviour.

References

Acquisti, A. and J. Grossklags (2005). "Privacy and rationality in individual decision making." *Security & Privacy, IEEE* 3 (1), 26–33.

Bansal, G., F. Zahedi, and D. Gefen (2010). "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online." *Decision Support Systems* 49 (2), 138–150.

Bauer, R. (1960). "Consumer Behavior as Risk Taking." in *Dynamic Marketing for a Changing World* Chicago: American Marketing Association, 389–398.

BCG (2013). The Value of Our Digital Identity *www.bcgperspectives.com* URL: https://www.bcgperspectives.com/content/articles/digital_economy_consumer_insight_value_of_our_digital_identity/ (visited on 29/06/2013).

Bélanger, F. (2012). "Theorizing in Information Systems Research using Focus Groups." *Australasian Journal of Information Systems* 17 (2).

Bélanger, F. and R.E. Crossler (2011). "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." *MIS Quarterly* 35 (4), 1017–1042.

Chen, J., W. Ping, Y. Xu, and B. Tan (2009). "Am I Afraid of My Peers? Understanding the Antecedents of Information Privacy Concerns in the Online Social Context." Presented at the Proceedings of the International Conference on Information Systems, Phoenix, Arizona.

Cunningham, S.M. (1967). "The major dimensions of perceived risk." *Risk taking and information handling in consumer behavior* 82–108.

Dinev, T. (2014). "Why would we care about privacy?." *European Journal of Information Systems* 23 (2), 97–102.

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

Dowling, G.R. (1986). "Perceived risk: the concept and its measurement." *Psychology & Marketing* 3 (3), 193–210.

Featherman, M.S. and P.A. Pavlou (2003). "Predicting E-Services Adoption: A Perceived Risk Facets Perspective." *International Journal of Human-Computer Studies* 59 (4), 451–474.

Fern, E.F. (2001). *Advanced Focus Group Research*. Sage publications.

Holton, J.A. (2007). "The coding process and its challenge." in Bryant, A. and Charmaz, K., eds., *The Sage Handbook of Grounded Theory* London: Sage Publications, 265–290.

Hong, W. and J.Y. Thong (2013). "Internet privacy concerns: an integrated conceptualization and four empirical studies." *MIS Quarterly* 37 (1), 275–298.

Jacoby, J. and L.B. Kaplan (1972). "The components of perceived risk." *Advances in consumer research* 3 (3), 382–383.

Jensen, C., C. Potts, and C. Jensen (2005). "Privacy Practices of Internet Users: Self-Reports Versus Observed Behavior." *International Journal of Human-Computer Studies* 63 (1), 203–227.

Lee, A.S. (1991). "Integrating Positivist and Interpretive Approaches to Organizational Research." *Organization science* 2 (4), 342–365.

Li, Y. (2011). "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework." *Communications of AIS* 28, 453–496.

Luo, X., H. Li, J. Zhang, and J.P. Shim (2010). "Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services." *Decision Support Systems* 49 (2), 222–234.

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

McAfee, A. and E. Brynjolfsson (2012). "Big data: the management revolution." *Harvard Business Review* 90 (10), 60.

Mitchell, V.-W. (1999). "Consumer perceived risk: conceptualisations and models." *European Journal of Marketing* 33 (1/2), 163–195.

Norberg, P.A., D.R. Horne, and D.A. Horne (2007). "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors." *Journal of Consumer Affairs* 41 (1), 100–126.

Preibusch, S. (2013). "Guide to measuring privacy concern: Review of survey and observational instruments." *International Journal of Human-Computer Studies* 71 (12), 1133–1143.

Sarker, S., A. Sahaym, and N. Bjorn-Andersen (2012). "Exploring Value Cocreation in Relationships Between an ERP Vendor and its Partners: A Revelatory Case Study." *MIS Quarterly* 36 (1), 317–338.

Sarker, S. and S. Sarker (2009). "Exploring Agility in Distributed Information Systems Development Teams: An Interpretive Study in an Offshoring Context." *Information Systems Research* 20 (3), 440–461.

Smith, H.J., T. Dinev, and H. Xu (2011). "Information Privacy Research: An Interdisciplinary Review." *MIS Quarterly* 35 (4), 989–1016.

Smith, H.J., S.J. Milberg, and S.J. Burke (1996). "Information Privacy: Measuring Individuals' Concerns About Organizational Practices." *MIS Quarterly* 20 (2), 167–196.

Son, J. and S. Kim (2008). "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model." *MIS Quarterly* 32 (3), 503–529.

Takeda, K. (2012). "User Identification and Tracking with online device fingerprints fusion." in *Security Technology (ICCST), 2012 IEEE International Carnahan Conference on* IEEE, 163–167.

TRUSTe (2013). 2013 TRUSTe US Consumer Confidence Index URL: http://www.truste.com/us-consumer-confidence-index-2013/ (visited on 07/08/2013).

Vodanovich, S., D. Sundaram, and M. Myers (2010). "Research Commentary—Digital Natives and Ubiquitous Information Systems." *Information Systems Research* 21 (4), 711–723.

Westin, A.F. (1967). *Privacy and Freedom*. New York, USA: Atheneum Press.