OPEN ACCESS
OPUS AUGSBURG

Universität Augsburg
Universitätsbibliothek

Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence

Sabrina Karwatzki, Manuel Trenz, Virpi Kristiina Tuunainen, Daniel Veit

Angaben zur Veröffentlichung / Publication details:

Karwatzki, Sabrina, Manuel Trenz, Virpi Kristiina Tuunainen, and Daniel Veit. 2017. "Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence." *European Journal of Information Systems* 26 (6): 688–715. https://doi.org/10.1057/s41303-017-0064-z.

Nutzungsbedingungen / Terms of use:

licgercopyright

Dieses Dokument wird unter folgenden Bedingungen zur Verfügung gestellt: / This document is made available under these conditions:
Deutsches Urheberrecht
Weitere Informationen finden Sie unter: / For more information see:
https://www.uni-augsburg.de/de/organisation/bibliothek/publizieren-zitieren-archivieren/publiz/

Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence

Sabrina Karwatzki[1], Manuel Trenz[1], Virpi Kristiina Tuunainen[2] and Daniel Veit[1]

[1] *University of Augsburg, Universitaetsstrasse 16, 86135 Augsburg, Germany;* [2] *Aalto University School of Business, Aalto, Finland*

Correspondence: Sabrina Karwatzki, University of Augsburg, Universitaetsstrasse 16, 86135 Augsburg, Germany.
Tel: +49 821 598-4083;
E-mail: sabrina.karwatzki@wiwi.uni-augsburg.de

Abstract
Organisations are highly interested in collecting and analysing customer data to enhance their service offerings and customer interaction. However, individuals increasingly fear how such practices may negatively affect them. Although previous studies have investigated individuals' concerns about information privacy practices, the adverse consequences people associate with external actors accessing their personal information remain unclear. To mitigate customers' fears, organisations need to know which adverse consequences individuals are afraid of and how to address those negative perceptions. To investigate this topic, we conducted 22 focus groups with 119 participants. We developed a comprehensive conceptualisation and categorisation of individuals' perceived adverse consequences of access to their information that includes seven types of consequences: psychological, social, career-related, physical, resource-related, prosecution-related, and freedom-related. Although individuals may limit their interactions with an organisation owing to consequences they associate with both the organisation and other actors, organisations can apply preventive and corrective mechanisms to mitigate some of these negative perceptions. However, organisations' scope of influence is limited and some fears may be mitigated only by individuals themselves or government regulation, if at all.
European Journal of Information Systems (2017) **26**(6), 688–715.
doi:10.1057/s41303-017-0064-z; published online 24 August 2017

Keywords: information privacy; access to individuals' information; perceived adverse consequences; mitigation mechanisms; focus group study

Introduction

Collection and analysis of large amounts of customer data is vital for the success of an increasing proportion of organisations. While at present only some business models are primarily founded on leveraging user data (such as Google and Facebook), most organisations have an interest in better understanding their current and prospective customers' behaviour and needs. This knowledge can inform their marketing campaigns, product and service offerings, and product innovation (Abbasi *et al*, 2016). As the Internet has become an integral part of both private and professional life, people today spend significant time online. They actively share a considerable amount of information with various services such as online shops or social networking sites. Moreover, they leave numerous data traces containing personal information about their

behaviour, preferences, and personality on the Internet. Therefore, to analyse their customers, organisations cannot only rely on information that individuals disclose to an organisation in direct interactions, but must also consider secondary data sources such as customers' search and browsing behaviour or their communication and interests displayed on social media sites (McKinsey & Company, 2013).

As collection and analysis of personal information often occurs without individuals' consent and awareness, people increasingly fear an infringement of their privacy (Kim *et al*, 2016). Surveys regularly show those negative perceptions: as an example, 88% of European and 89% of US adults reported worrying about their online privacy (TRUSTe, 2013; BCG, 2013). Furthermore, 59% of Europeans said that they had experienced severe data breaches, including stolen bank account information, online identity theft, or hacked social media accounts (Symantec, 2015). People take possible consequences into account when deciding on their online activities, such as whether and how to interact with a service. For example, a recent survey showed that approximately two-thirds of German customers would decide against using services that require disclosure of personal information such as their real name or date of birth (BITKOM, 2015). Thus, understanding perceptions of threat is crucial for organisations.

Nevertheless, no prior study has systematically identified the adverse consequences that access to personal information may trigger nor has it been investigated how these consequences can be mitigated. The most frequently used privacy-related concept of privacy concerns refers to the extent of worries individuals have with respect to how others handle their personal information (Hong & Thong, 2013). Based on this conceptualisation, previous studies have identified how privacy fears may be alleviated by offering highly beneficial services such as convenient shopping or the ability to easily communicate with friends via social network sites (Krasnova *et al*, 2010; Posey *et al*, 2010; Jiang *et al*, 2013). Other studies have investigated how organisations can attempt to build trust, for example through displaying seals or privacy notices (Hui *et al*, 2007; Tsai *et al*, 2011; Kim *et al*, 2016). However, research of such strategies has been unable to stop the growing resistance to information access. Complementary perspectives on information privacy may uncover different approaches to this issue (Bélanger & Crossler, 2011; Preibusch, 2013; Dinev, 2014), for instance by reducing the sources of perceived adverse consequences or by directly targeting customers' privacy fears. Direct assessment and different tactics to mitigate adverse consequences have been shown to be effective in, for example, consumer behaviour and psychology studies (Meichenbaum, 1977; Lazarus & Folkman, 1984; Featherman & Pavlou, 2003; Luo *et al*, 2010), but the specific adverse consequences that individuals fear when their information is accessed are still largely unidentified. In an age where data are one of the most powerful resources of many organisations (Abbasi *et al*, 2016), a detailed understanding of customers' resulting fears would allow organisations to design and tailor mechanisms that sufficiently mitigate them.

Given all these considerations, we pose the following research question: *What are individuals' perceived adverse consequences of access to their information and what is the scope of organisational influence on these consequences?*

This research question translates into three research objectives. (1) We aim to uncover individuals' perceptions of the adverse consequences of access to their information. By empirically identifying the possible adverse consequences that individuals might have, we intend to provide a conceptualisation and categorisation of these consequences. (2) We build on this comprehensive categorisation to examine which actors individuals associate with these feared consequences. In particular, we seek to better understand which consequences may derive from the organisation itself and which consequences may be caused by other actors. (3) We analyse how perceptions about adverse consequences can be mitigated and what role organisations can play in addressing this variety of adverse consequences. To uncover these individual perceptions, we conducted a series of focus group discussions.

Research foundations

Our review of prior studies revealed that research has not yet thoroughly investigated individuals' perceived adverse consequences of third-party access to their information. We therefore ground our research on prior literature on established privacy-related concepts and on adverse consequences that were conceptualised outside of privacy research. After providing a cognate-based definition of information privacy, we review the most frequently applied privacy-related conceptualisations of privacy concerns and privacy risks, discuss their limitations in the light of our research objectives, and infer the necessity for a complementary perspective. We then review broader conceptualisations of risk that have been used outside of privacy research and discuss the extent to which these can inform our pre-understanding of perceived adverse consequences of information access.

Information privacy, established privacy-related concepts, and their limitations

In general, while research on privacy has been conducted in a variety of fields, consensus is lacking amongst philosophy, psychology, sociology, and legal scholars about the exact nature of privacy (Smith *et al*, 2011). As we are interested in investigating individuals' perceptions of how access to their information may negatively affect them, we base our understanding of privacy on the cognate-based conceptualisation of privacy. This conceptualisation relates privacy to individuals' minds and perceptions (Westin, 1967; Altman, 1975), while value-based definitions conceptualise privacy as a societal moral value or norm (Smith *et al*, 2011).

Information privacy is the subset of general privacy on which privacy-related information systems research concentrates (Bélanger & Crossler, 2011). The emergence of this focus can be explained by the advent of digitized communication, the extensive storage of private information, and the availability of advanced information technologies to aggregate and analyse large volumes of information, all of which have led to questions about the influence individuals still possess over the acquisition and use of their personal information. As we aim to investigate which adverse consequences individuals perceive to potentially occur once personal information might be accessible by other actors, we define information privacy as "an individual's self-assessed state in which external [actors] have limited access to information about him or her" (Dinev *et al*, 2013, p. 299). Availability of personal information to external actors automatically implies a loss of privacy because access to this information is no longer restricted. This information is then also subject to potential misuse, which may result in adverse consequences for the individual.

Following Smith *et al* (2011) and Dinev *et al* (2013), we use "privacy" to refer to information privacy for the remainder of the paper. To provide an overview of the current state of the literature on adverse consequences of information access, we look at two related concepts that previous studies have used extensively: privacy concerns and privacy risks.

Privacy concerns As measuring privacy itself has been deemed nearly impossible (Smith *et al*, 2011), privacy concerns have evolved as a common proxy for privacy (Xu *et al*, 2011; Smith *et al*, 2011; Dinev *et al*, 2013). While many conceptualisations of privacy concerns exist (Smith *et al*, 1996; Malhotra *et al*, 2004; Dinev & Hart, 2006) and have been used in various contexts, they all typically refer to concerns surrounding how specific parties access and use personal data. Hong and Thong (2013) summarised and integrated previous research on privacy concerns and define them as "an individual's perceptions of his or her concern for how personal information is handled" (p. 276) by external actors. Privacy concerns comprise six dimensions that commonly appear in extant literature. These concerns relate to the collection of personal information; the secondary, unauthorised use of personal information; the improper access of personal information by people not authorised to see and work with the information; errors in personal information; control over one's personal information; and one's awareness of information privacy practices of external actors (Hong & Thong, 2013).

For the purposes of our study, the concept of privacy concerns is too vague. While it captures how and why one's information may be accessed by others and how it may be misused, it does not indicate any of the specific adverse consequences individuals perceive to potentially arise from a privacy invasion. None of the dimensions refers to a specific adverse consequence *per se*. While events such as collection and improper access can be a source or trigger for adverse consequences, negative outcomes for individuals remain nonspecific.

Privacy risks Privacy risks have been conceptualised in two ways. Firstly, they have been defined as opportunistic behaviour related to the release of personal information leading to a loss of control (Dinev & Hart, 2006; van Slyke *et al*, 2006; Wu *et al*, 2009; Chiu *et al*, 2014). As this conceptualisation closely resembles privacy concerns, it does not allow for the derivation of new insights into perceived adverse consequences associated with access to individuals' information. Secondly, privacy risks have been defined as the expectation of a high potential for loss or negative outcomes associated with the release of personal information (Malhotra *et al*, 2004; Xu *et al*, 2011; Smith *et al*, 2011; Dinev *et al*, 2013). This conceptualisation focuses on adverse consequences, but it is unidimensional and fairly abstract. It covers potential losses and negative outcomes in general, but lacks in-depth specification of the loss or other kinds of negative outcomes referred to in the definition. In other words, it remains unclear which adverse consequences individuals may perceive to occur if and when information is accessed by other actors. Only one specific facet, adverse social consequences, has received some attention in very few studies that have investigated social interactions of individuals (Petronio, 2002; Krasnova *et al*, 2009). Some consequences have been cited in earlier literature, including emotional, material, and physical consequences (Smith *et al*, 2011), and in more detailed level social discrimination, manipulation, coercion, and censorship (Acquisti *et al*, 2015), but a systematic investigation has been missing to date.

Thus, the current understanding of the perceived adverse consequences of access to individuals' information is very limited. However, as the concept of risk has been extensively studied in related disciplines, such as psychology and consumer behaviour, these findings may guide our inquiry to adverse consequences in the privacy context.

Risk in other contexts

In general terms, risk is commonly defined as a function of (1) the adverse consequences of a situation, referring to the negative outcomes of a situation, and (2) the likelihood of their occurrence (Cunningham, 1967; Jacoby & Kaplan, 1972; Dowling, 1986; Mitchell, 1999). Risk has often been defined as a multifaceted concept, even though some debate has occurred as to the precise nature of the various risk facets (Dowling, 1986). Additionally, these facets are highly context-dependent, as different risks may be present in different situations (Dowling, 1986). Frequently cited facets of risk include performance, social, physical, financial, and psychological risk (Jacoby & Kaplan, 1972; Dowling, 1986; Mitchell, 1999). These facets are depicted in Table 1.

This differentiated perspective of risk has proven useful in explaining consumer behaviour in domains such as information systems, marketing, and psychology

Table 1 Different facets of risk (Jacoby & Kaplan, 1972; Dowling, 1986; Mitchell, 1999)

Facet of risk	*Description: The chances that the outcome of a situation…*
Performance risk	… is not of expected quality
Social risk	… negatively affects how others think about a person
Physical risk	… negatively affects a person's safety (i.e. may be harmful or injurious to health)
Financial risk	… leads to monetary loss
Psychological risk	… negatively affects a person's peace of mind or self-perception

(Featherman & Pavlou, 2003; Luo *et al*, 2010). While it is beyond the scope of our study to estimate the probabilities of the occurrence of adverse consequences associated with external actors who have access to individuals' information, the general risk literature provides us with a sound understanding of the different types of consequences that have been observed in other contexts.

In summary, the adverse consequences individuals perceive to arise from access to their information have not been studied in detail, yet. Literature on privacy concerns provides insights into individuals' perceptions on how and why information may be accessed and misused, but remains vague about which consequences may arise from data collection and misuse. Privacy risks have been either conceptualised as opportunistic behaviour related to the release of personal information or have been treated as a unidimensional perception of expected losses arising from the release of personal information. Such an abstract unidimensional conceptualisation does not guide an investigation of what individuals specifically fear and thus does not allow the derivation of suitable mitigation mechanisms for organisations. Even if we can find a more elaborated differentiation of risk facets in other contexts, these facets of risk are known to be context-specific (Dowling, 1986; Featherman & Pavlou, 2003), and none, so far, is specific to privacy. The applicability of established risk dimensions remains unclear and may overlook risk facets that relate to privacy-specific adverse consequences. Therefore, we will discuss the nature of perceived adverse consequences of access to information next. Based on this pre-understanding, we then explore the different types of perceived consequences and how individuals' fears of such consequences could be mitigated.

The nature of perceived adverse consequences of access to individuals' information

In accordance with the general risk literature (Glover & Benbasat, 2010), we refer to adverse consequences of access to an individual's information as the individual's perception of potential negative outcomes from other actors' access to that information. As described above, combining adverse consequences with their perceived likelihood of occurrence would result in an individual's perceived risk associated with access to information. Studies seeking to quantify the risks of access to individuals' information in specific contexts would require an in-depth understanding of all possible adverse consequences. In this light and in line with prior studies on privacy, we focus on perceived rather than actual adverse consequences. Perceived and actual consequences differ in many ways, most importantly in their relevance to an individual's decision on how to behave: perceived adverse consequences are the subjective view of which negative outcomes may occur. An individual thereby accounts for his or her perception about who has access to which personal information and his or her perception of how this personal information could be used in a harmful way. Actual consequences, on the other hand, are the consequences that actually occur once certain information has been accessed by a given actor. Because of information asymmetries (e.g. data collected or passed on without the individual's knowledge), but also owing to incorrect assessment of external actors' involvement and interests, perceived adverse consequences may be considerably different from actual consequences. The perceptions of adverse consequences shape an individual's expectations and related behaviour at a time when consequences have not yet occurred, but the fear of those consequences may lead to preventive actions or coping strategies. Actual consequences, however, may only trigger a behavioural reaction once they occur in reality (Bauer, 1960; Glover & Benbasat, 2010).

Studies on information practices have primarily focused on the information-requesting party, such as service providing organisations or peers in a social network (e.g. Xu *et al*, 2009; Posey *et al*, 2010; Anderson & Agarwal, 2011; Dinev *et al*, 2013). Yet, a much wider set of actors may gain access to an individual's information and trigger adverse consequences. In addition to the organisation as receiver of purposefully disclosed personal information, several secondary actors, including third-party organisations, governmental agencies, and illegal entities, may gain access to personal information (Conger *et al*, 2013). Also, these organisations may collect additional personal information before, during, and after a transaction, all unbeknownst to the customer (Conger *et al*, 2013).

Since our investigation extends beyond the interactions between organisations and individuals to include all circumstances under which other actors may gain access to personal information, we include individuals' private and professional contacts in our overview. Private contacts are often direct receivers of personal information, as on social networks and in personal communication (Krasnova *et al*, 2010), but may also be a source of

Table 2 Actors that may gain access to personal information (based on Chen *et al*, 2009; Sánchez Abril *et al*, 2012; Conger *et al*, 2013)

Actor	*Explanation*	*Type of information access*
Focal organisation (service provider)	Primarily firms, but also non-profit or governmental organisations that offer specific services, such as online shops, online banking, citizen services, apps, social network sites, etc.	*Actively shared access*[a] Primary interaction partner in most situations. Service provider is the intended receiver of personal information, which is used to enable a service. *Unintended access*[b] Focal organisation may track additional customer data before, during, and after an interaction with a customer At times, the service provider provides only a platform for others to interact (e.g. social network sites) and is thus not the intended receiver of information shared via this platform, yet may also access all information.
Third-party organisations	Organisations (mostly firms) that are not the direct interaction partner in a transaction.	*Mostly unintended access*[b] Focal organisations share information with third-party organisations (sometimes legally required, e.g. for credit assessment, but even if made transparent to a customer, those third parties often fade into the ubiquity of the transaction process); third-party organisations may also track customers where data collection may not relate to any transaction.
Private contacts	Relatives, friends, and acquaintances.	*Actively shared access*[a] *and unintended access*[b] Can be primary interaction partner (on social network sites and in other forms of social interaction), but may also gain unwanted access to personal information.
Professional contacts	(Potential) employers, colleagues, and other business contacts.	*Actively shared access*[a] *and unintended access*[b] Individuals may directly interact with professional contacts in professional social networks, but individuals typically fear that professional contacts will search for information about prospective employees or gain access to compromising information in already-existing employment relationships.
Intelligence services	Governmental agencies that collect and analyse information in support of law enforcement and national security.	*Unintended access*[b] *only,* e.g. owing to surveillance.
Criminals	Third parties with bad intentions, e.g. monetary theft.	*Unintended access*[b] *only,* e.g. owing to hacking into an individual's account or intercepting the information flow between an individual and an organisation.

[a]An *individual* gives an actor access to personal information for a specific purpose, but this information may be subject to unintended use.

[b]An *actor* may gain unintended access to individuals' information by surreptitiously collecting, buying, or stealing an individual's information.

risk (Chen *et al*, 2009). Professional contacts comprise employers and colleagues and can be associated with adverse consequences if they gain access to certain types of personal information (Sánchez Abril *et al*, 2012). Table 2 provides a characterisation of all relevant actors which may gain access to an individual's information.

Research method

To understand the scope of organisational influence, we aim to uncover the perceived adverse consequences of access to individuals' information and to identify the associated actors. To this end, we have chosen an interpretive research approach with exploratory focus groups to answer our research question. Focus groups are particularly well suited to achieve our research goals for two reasons. First, they can be used to identify, collect, and explain individual feelings, thoughts, and behaviours. Thus, they are especially suited for uncovering and developing a deeper understanding of people's perceptions and cognitions (Miltgen & Peyrat-Guillard, 2014). Making such everyday knowledge and experiences explicit allows to generate theoretical constructs and understand their relationships (Fern, 2001). Second, focus groups are a powerful method for "trying to obtain a deeper understanding of constructs (i.e. their dimensions)" (Bélanger, 2012, p. 111) by encouraging participants to interact with each other. This interaction fosters the exchange of participants' ideas, thoughts, and anecdotes and also triggers a clarification process between participants as they comment on each other's points of view and critically question opinions (Stewart *et al*, 2007). This process allows researchers to gain in-depth insights that cannot be fully obtained in one-on-one interviews (Kitzinger, 1995).

Focus group set-up

We designed our focus groups according to guidelines of Fern (2001). Altogether, we conducted 22 focus groups with a total of 119 people (on average 5–6 participants in each group; see "Appendix A"). Every individual who can engage in Internet activities is a decision maker regarding his or her privacy and has perceptions about privacy in an online context. Thus, these individuals serve as experts in our focus groups. We sought across-group heterogeneity and within-group homogeneity to balance two otherwise contradictory goals: collecting insights from many different perspectives to ensure that no interesting findings are missed, while preserving a homogeneous environment that fostered openness to sharing experiences that are as rich and detailed as possible (Fern, 2001). To achieve heterogeneity, we recruited participants who varied widely in age (well distributed between 13 and 71), gender, Internet affinity, and experiences, providing a fair approximation of general Internet users (albeit not representative in a statistical sense). Participants included professionals, students, employees, executive staff, and management and held diverse occupations, such as psychoanalysts, medical sector employees, farmers, sales representatives, office assistants, consultants, engineers, mechanics, journalists, bankers, teachers, and clerical staff. To foster a fruitful discussion, homogeneity needs to exist in terms of background but not attitudes (Barbour, 2008). Therefore, we created focus groups where the within-group composition was as homogeneous as possible with regard to age, educational background, and social status so that people felt uninhibited in sharing their experiences and perceptions.

Conduct of focus groups

The 22 focus groups were conducted between June 2014 and November 2015 in Germany, which is exemplary of a highly developed economy with high Internet penetration. We relied on the guidelines of Fern (2001) with respect to duration, setting, moderation, and design of our semi-structured interview guide. The focus group sessions lasted between 40 and 105 minutes, with an average length of 75 minutes. Three moderators conducted the focus groups, with each one using a semi-structured interview guide (see "Appendix B") and detailed guidelines to ensure consistency. The interview guide provided the moderators with initial guidance, but also allowed for flexibility in accommodating each group's unique aspects and in exploring new and unexpected ideas. We encouraged our participants to share in depth which activities they perform online, along with how and why they decided to disclose or not to disclose particular information to specific organisations and individuals online; which fears they generally have when their information can be accessed by other parties; and what expectations they have regarding the mitigation of adverse consequences.

Analysis

We recorded and transcribed all focus group discussions, leading to over 700 pages of transcription from the 119 focus group participants. Our subsequent data analysis comprised several steps. We performed an iterative analysis using open and axial coding (Corbin & Strauss, 1990; Sarker & Sarker, 2009) supported by the software Atlas.ti. For open coding, we compared actions, opinions, and thoughts that our participants mentioned and identified similarities and differences. We labelled all statements that referred to perceptions about any negative outcomes that may arise from information being accessed by external actors with a short summary of their content. We also coded all text passages in which participants talked about specific actors and mitigation mechanisms. As a starting point, we used our understanding of perceived adverse consequences from other contexts as well as the presented overview of actors, but did not limit our coding to these categories (Walsham, 1995). Open coding was performed independently by the first author and a well-trained and experienced research assistant. It was accompanied by ongoing discussions and comparison of codes with dual meanings to ensure a common understanding of the data (Strong & Volkoff, 2010).

For axial coding, we related subcategories to categories and investigated the relationship between the categories. Subcategories that had a common theme were critically compared and contrasted before we decided on whether to generalise them by adding them to a joint category. We then mapped the perceptions of consequences to the various actors individuals thought might cause them and derived a comprehensive framework showing who might mitigate consequences and how this mitigation might be done. "Appendix C" presents an example of a passage from our focus groups and illustrates how we applied open and axial coding to this passage. We also carefully compared data across our heterogeneous groups to see if any patterns emerged. While not all focus groups discussed all types of consequences, actors, and mitigation mechanisms, we detected no systematic deviations with respect to age, educational background, or gender (see "Appendix H").

Evaluative and trustworthiness criteria

The criteria developed by Parks *et al* (2016) guided the evaluation of our interpretive research approach. They suggest to ensure (1) the trustworthiness (Lincoln & Guba, 1985) and (2) the adequacy of the research process and its empirical grounding (Corbin & Strauss, 2008), as those criteria are equally important as the criteria of internal or external validity, reliability, and objectivity are in positivist research (Lincoln & Guba, 1985; Parks *et al*, 2016).

The trustworthiness of our study's findings is ensured through the criteria of credibility, transferability, dependability, and confirmability (Lincoln & Guba, 1985). Their assessment indicates that our results are believable, can

be transferred to other contexts, and are consistent and confirmable. A detailed appraisal of each criterion can be found in "Appendix D".

We adopt the criteria by Corbin and Strauss (2008) to help the reader judging the adequacy of the empirical grounding and the research process. The documentation of the empirical grounding indicates how the data revealed the conceptualisation of adverse consequences and its linkages. A detailed overview of all criteria and their appraisal is provided in "Appendix E". The adequacy of the research process is, amongst others, signified by the established procedures that guided sample selection and emergence of categories. We provide detailed information on evaluative criteria of the research process in "Appendix F".

Findings

In the following, we present our findings, beginning with the conceptualisation and categorisation of perceived adverse consequences of information access. We continue with determining which actors participants see as potential sources of these adverse consequences and discuss how they can be mitigated.

Perceived adverse consequences of access to individuals' information

Our analysis revealed seven categories of consequences that individuals perceive: physical, social, resource-related, psychological, prosecution-related, career-related, and freedom-related (see Table 3).

Physical consequences Physical consequences are the most tangible type of possible outcomes. They comprise all perceived consequences resulting from access to individuals' information that could harm a person's physical well-being. Our focus groups revealed three manifestations of physical harm that participants feared. *Physical violence* is a possibility because information about a person's whereabouts can be obtained to seek a person out. For example, information about a person's address, habits, or plans can be used by someone wanting to hurt that person, and the Internet facilitates access to such information. In addition, individuals are afraid that access to their information can make them more vulnerable to *stalking*. The Internet not only helps stalkers track and find personal information about their targets but also to initiate contact with them and exercise some form of psychological violence, which in extreme cases can culminate in physical violence. Another manifestation of physical consequences is *kidnapping and imprisonment*. On the one hand, personal information can be used to facilitate kidnapping, either because possible victims deemed worth being kidnapped can be identified or because criminals have information about people's whereabouts. On the other hand, people who make use of the Internet's possibilities to conveniently express their views and reach an audience can also be easily identified. This knowledge about people with divergent opinions and attitudes can, in the most extreme case, lead to physical violence or forcible confinement, for instance by governments in non-democratic systems wanting to suppress those opinions. Table 4 depicts illustrative quotes from our focus groups for all manifestations of physical consequences.

Social consequences Social consequences refer to changes in a person's social relationships that can negatively affect the individual's status within a social group. Our focus group participants believe that social consequences can be induced in several ways: either other people intentionally or unintentionally release information about an individual that leads to social consequences, or individuals disclose personal information themselves but only become aware of adverse effects afterwards. We found three manifestations of social consequences. The first, *condemnation*, can occur when others form a dismissive opinion about a person. Such a disadvantageous judgement can be based on information about someone's opinions, views, habits, lifestyle, and behaviour. It can lead to embarrassment and loss of reputation and respectability. Even though certain information might be accurate, as such, individuals are often afraid that others may form an unfavourable opinion based on incomplete information and "pigeonhole thinking". If other people spread disparaging information about others on purpose, the adverse consequences of *slander and bullying* may arise. On the Internet, such offending and discrediting messages can be communicated quickly and efficiently. The third form of social consequences can be summarised as *social conflict*. The release of personal information can lead to disputes if others find a person's opinions or behaviour perplexing or if they are disappointed by, annoyed at, or hurt by a person. Evidence for the three manifestations is provided in Table 5.

Table 3 Categories of perceived adverse consequences of access to individuals' information

Category	*Definition*
Physical	Loss of physical safety owing to access to individuals' information
Social	Change in social status owing to access to individuals' information
Resource-related	Loss of resources owing to access to individuals' information
Psychological	Negative impact on one's peace of mind owing to access to individuals' information
Prosecution-related	Legal actions taken against an individual owing to access to individuals' information
Career-related	Negative impacts on one's career owing to access to individuals' information
Freedom-related	Loss of freedom of opinion and behaviour owing to access to individuals' information

Table 4 Manifestations and illustrations of physical consequences

Manifestations	*Illustrative quotes from focus groups*
Physical violence	"I was once threatened by someone via Facebook. I was extremely glad that I hadn't shared any sensitive data online. I was in a state of panic because if my exact residence or real name or other things like that had been available, it would have been much easier to find me in a city not too big such as Munich." (P4, FG10)
Stalking	"I think you are a little bit more vulnerable. I've heard of cases, for example, where stalkers used information that can be accessed via the Internet. And then they know where you live, what you do all day long, your habits, etc. It offers individuals with such predilections a platform to locate people." (P2, FG7)
Kidnapping and imprisonment	"Adidas and Nike offer this Runtastic-App […]. There are so many people that take their smartphone with them and enable GPS to track their route, and then they have all the data about your run: running style, which route, pace, distance, how often you run." (P1, FG12) "Yes, but that's not all. Imagine someone is stalking you and notices that you are using this app and successfully hacks into your device. I mean, nowadays it does not take too much to hack into mobile devices for people who really want to do this. And then this person says, well ok, every Monday at half past five in the morning, his target is jogging in the forest and then this person might be abducted quickly." (P2, FG12)

Table 5 Manifestations and illustrations of social consequences

Manifestations	*Illustrative quotes from focus groups*
Condemnation	"I've lately googled myself […]. The first hit I got was a comment I made about some American beer 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." Later: "When I think back how I behaved five years ago and compare it with today, I don't want others to see these pictures now. I want to freely develop over time, without being locked into a stereotype." (P4, FG9)
Slander and bullying	"[Bullying] is really bad and the reason why I'm not on Facebook. It is nothing but my own business what I've eaten, where I've been, what I've done, what movies I love, and all this other crap. And someone else might bully you for your hobbies or for all the stuff you do." (P5, FG20)
Social conflict	"You just get tagged to activities. For instance, a friend of mine is living in Australia and she was having a party and was really drunk. Her friends recorded a video and uploaded it to the Internet. Her parents are also on Facebook, of course, and she got into serious trouble. Her parents said that they finance her life down there and she just boozes. Her parents stopped sending her money. After that, she published a text on Facebook and complained about the behaviour of her friends, that they should not do something like that." (P5, FG14)

Resource-related consequences Resource-related consequences deal with the loss of different types of resources and can be tangible or intangible. In particular, we found evidence of consequences related to temporal, financial, and material resources. People are afraid of a *time loss* when they have to deal with annoying but otherwise harmless outcomes of information abuse, such as time spent deleting spam e-mails. Regarding financial resources, we distinguish between *direct and indirect financial loss*. Individuals frequently mentioned fearing direct loss of money because they had shared their bank account details or payment information somewhere on the Internet and this information could be misused. Indirect financial losses can occur if personal information, such as health or behavioural information, is exploited for price discrimination in services and products. For example, a private health insurance company might collect information from fitness apps about whether its customers exercise regularly and adjust their insurance rates accordingly. *Material loss*, the damage to or stealing of tangible objects, was brought up by the focus group participants particularly in the context of burglaries, which may happen when the availability of information about people's property and their absence from home is used by criminals. See Table 6 for illustrative quotes from our focus groups.

Psychological consequences Psychological consequences comprise all outcomes where someone's peace of mind is negatively affected as a result of access to a person's information. These consequences relate to a mental discomfort that individuals fear being troubled with. They are internal and cannot be observed, as such. We distinguish three manifestations of psychological consequences. A *mental discomfort caused by surveillance* is experienced by individuals who fear that all activity they perform on the Internet is monitored. Perceived constant surveillance can make people uneasy and uncomfortable, even if they believe that they have done nothing wrong. People also feel a *mental discomfort caused by unknown consequences*. The sheer amount of data collected makes people anxious about what organisations could potentially do with this information. Even if they cannot imagine any concrete harmful effects for the time being, they are afraid of adverse consequences at a later time. The third manifestation of psychological consequences is *mental*

Table 6 Manifestations and illustrations of resource-related consequences

Manifestations	*Illustrative quotes from focus groups*
Time loss	"Once we booked a room in the Maritim Hotel, and now we always get special offers for the Maritim Hotel. Everywhere you booked something, it gets back to you. And this cannot be stopped. […]" (P6, FG22) "This is also true for booking.com and Airbnb. You are bombarded with the newest offers. And now I have to… my daily task is to work through 20, 30 mails." (P1, FG22)
Financial loss (direct and indirect)	*Direct:* "Regarding online shopping in a private context, my biggest concern is that my account information is stolen and that consequently a huge amount of money is debited." (P3, FG8) *Indirect:* "They save all this information. For instance, they record which diseases I'll inform myself about, which drugs I buy. And I've read a report or saw it on TV that American insurance companies are already using this, that they say, whoever googled this on the Internet probably has this disease and thus they'll classify him accordingly within their insurance policies." (P1, FG19)
Material loss	"If someone had a profile of all my expenses, I would be afraid that he knows, ah, now she has booked holidays for this and that week and thus is not at home. Criminals might then also know that the flat is vacant." (P2, FG8)

Table 7 Manifestations and illustrations of psychological consequences

Manifestations	*Illustrative quotes from focus groups*
Mental discomfort caused by potential surveillance	"I also think, as you said, that anyone can get access to your data. Facebook and WhatsApp might support that; they can sell your data. Due to this, everyone can be monitored, not only by firms but also by governments. For instance, the USA can see everything that we do. Frankly, this is really worrying me, that I, as a normal citizen, can be completely under surveillance, without laws that protect you since the Internet is kind of an anarchic system in the USA. If the servers are located in the USA, you really can't do anything." (P3, FG7)
Mental discomfort caused by unknown consequences	"This is difficult for me, because on the one hand it is so wrong that they use your information. But on the other hand, I think, what bad things could they do with it? It is so difficult to grasp that." (P6, FG14) "This risk that something will come out of that, it's developing, it's rising…" (P4, FG14)
Mental discomfort caused by loss of control	"I often think that everyone makes missteps in their youth and this might also be available on Facebook or on the Internet in general. If our parents did something stupid, it was forgotten five years later, but for us, it theoretically – or not only theoretically – but there is really the possibility that this will pop up again in 40 years, if an unfavourable picture about you that had been uploaded, whether you wanted that to happen or not, whether you carefully considered that or not. This really frightens me and it restricts us in our freedom to do what we love to do." (P5, FG3)

discomfort caused by loss of control. People are worried that once information about them is available online, they cannot control who can access it and how this information will be used. Moreover, people worry that deleted information never fully disappears from the Internet. We provide illustrative quotes for the manifestations of psychological consequences in Table 7.

Prosecution-related consequences Prosecution-related consequences comprise legal actions that may be taken against an individual because of information disclosure. Two manifestations of prosecution-related consequences emerged from our data: *unlawful criminal prosecution* and *lawful criminal prosecution*. *Unlawful criminal prosecution* occurs when an individual is wrongfully accused. We found two instances that may cause such an unlawful prosecution: identity theft and false suspicion. Identity theft refers to the use of a person's identity to deliberately perform illegal actions, such as fraud or other crimes, while impersonating this individual. Typically, personal information such as name, identifying numbers, or credit card information is misused. Individuals fear this consequence because they may end up liable for the identity thief's actions and may be prosecuted. A person can also be falsely under suspicion. Certain information about a person can become available or may be posted online on purpose to mislead authorities and cause suspicion that this individual has committed a crime. However, personal information can also be used to hold people liable for any illegal activities that they actually have performed, which results in a *lawful criminal prosecution*. The traceability of online activities makes it more difficult for individuals to hide unlawful behaviour, such as illegally downloading music or videos. Evidence for these manifestations can be found in Table 8.

Career-related consequences Career-related consequences refer to hampered career development. This negative impact can occur when different types of personal information are available to employers. For example, information might let employers assume that a person is not suitable to represent an organisation, does not have the necessary skills to do a good job, or is not loyal to the employer. This harm manifests in three forms, which depend on when this information becomes available to the employer and on the perceived severity of the

Table 8 Manifestations and illustrations of prosecution-related consequences

Manifestations	*Illustrative quotes from focus groups*
Unlawful criminal prosecution	"I am just scared that one day the police will stand in front of me and say, you have done this and that. Then I say: that is not possible. [Then they answer:] no we have pictures here, you were captured with this camera, and you were logged in there, so you must have been there, so you've had time. And that I am just not able to prove my innocence because with the disclosed data it can be set up in that way." (P5, FG14)
Lawful criminal prosecution	"I've never streamed something illegally or anything similar. […] I didn't dare to do it because I was always afraid that they cache data about that and then there is a lawsuit against me." (P2, FG6)

Table 9 Manifestations and illustrations of career-related consequences

Manifestations	*Illustrative quotes from focus groups*
Not getting hired	"If you search for my name, you find out how I was ten years ago. This might be not so advantageous if your employer is searching for you [on the web] and then stumbles upon stuff you did. Not so cool. So that should not be available on YouTube." (P3, FG8)
Not being promoted	"Let me say this, if they know where we are, for example the employer, you can make a bad impression if he sees that, I don't know, you called in sick, and he sees pictures of you sitting in a café or something similar." (P4, FG11)
Being fired	"No, that can happen very fast. I saw a screenshot yesterday. A girl agitated against an asylum seeker. One month later, she posted: 'Yes, I got a job at the German armed forces!' Then someone made two screen shots and sent them to the armed forces and one day later the post had 20,000 likes and of course, she was no longer wanted by her employer." (P3, FG12)

information. Accordingly, individuals are afraid that certain information may lead to *not getting hired* if they are looking for a new job. If they are employed, degrading information may result in *not being promoted* or even *being fired*. Table 9 exhibits quotes from our focus groups that exemplify these three manifestations.

Freedom-related consequences Freedom-related consequences comprise all outcomes that describe a manipulation or restriction of an individual's opinion and behaviour. Thus, these consequences refer to limitations on an individual's freedom and uninfluenced decision-making, which result in fear that the person is no longer acting independently when forming an opinion or behaving. Detecting the actual occurrence of such consequences may be challenging, as the outcome is intangible, difficult to determine and observe, and often the result of a long-term, unconscious, gradual process. Three manifestations of freedom-related consequences emerged from our data. *Manipulated opinion* refers to third parties who influence an individual's forming of an opinion. For example, information can be selectively presented so that it aligns with a third party's objectives while unfavourable information is filtered out. Having extensive knowledge about what motivates a person can help with this type of manipulation. *Manipulated behaviour* is associated with the use of information to influence an individual's decisions. For example, participants in our focus groups recounted companies that try to influence consumers' purchasing decisions by anticipating customers' preferences, needs, and willingness to pay. *Restricted behaviour* refers to the limited options available to an individual because third parties are not willing to offer a full set of choices owing to their knowledge about the given person. For example, a disability insurance company may not want to insure a person if it knows the person's family medical history. Example quotes from our focus groups are presented in Table 10.

Perceived adverse consequences of access to individuals' information, associated actors, and mitigation mechanisms

To be able to address individuals' perceptions of adverse consequences, it is necessary to first understand whom individuals see as the source of these consequences. This information can then be used to develop strategies to mitigate specific customer fears either by influencing the actors' behaviour, rectifying the perceptions, or alleviating the severity of the consequences. We rely on the categorisation of actors outlined in the research foundations section and utilise the in-depth information gathered from the focus groups to map perceived consequences to these actors (see "Appendix G").

Our focus group data indicate that organisations that have direct contact with an individual seem to be associated with only three of the seven consequences that we uncovered. Most consequences are simultaneously or exclusively caused by other actors that the organisation can barely influence. Focal organisations are associated with psychological consequences because individuals associate mental discomfort with the vast amount of data organisations collect and analyse. Moreover, resource-related consequences, in particular temporal and indirect financial losses, as well as freedom-related consequences are derived from individuals' beliefs that organisations want to direct consumers into buying their products and services to generate profits.

Table 10 Manifestations and illustrations of freedom-related consequences

Manifestations	*Illustrative quotes from focus groups*
Manipulated opinion	"For example, when I run a Google search query, they save the whole search history, and if they now want to influence which information I'll see about a current topic then they could severely restrict that. Thus, we're coming back to the topic 'government.' If one government applies pressure or sets incentives for Google to censor something or to influence the opinions of certain people, then I think that is a very real threat." (P3, FG8)
Manipulated behaviour	"In the first step, we can observe that if I google lawnmowers, I'll get a lot of offers for lawnmowers in the following days. That's what happens right now. I think in the next step, if it is really possible, that they will bring up the idea of buying a new lawnmower a month before I'll need it, just because your last purchase of a lawnmower has been two years ago or because you just bought another gardening tool, or whatever. So they steer you towards a purchase." (P3, FG10)
Restricted behaviour	"You might not know what they do with your data, e.g. insurance companies. At some point in time, you might be in the situation where you don't get life insurance anymore, even though you want to have it, and it is not transparent why that is the case. […] They might have somehow collected additional information about your health status." (P5, FG13)

Private contacts with harmful intentions can be a source of physical consequences as well as a source of psychological consequences, as individuals can be uncomfortable when everything they do is visible to others they know. Moreover, private contacts are largely responsible for social consequences: individuals have personal interactions with their private contacts and thus might fear changes in their social status. However, professional contacts are associated with social consequences as well, as individuals also fear damaging their social relationships with colleagues and other work-related contacts. Career-related consequences are driven solely by professional contacts, especially current and future employers or other business contacts, as they can influence a person's career.

Moreover, individuals associate the same consequences with third-party organisations as with organisations that constitute the direct interaction partner. These are essentially resource-related and freedom-related consequences, because individuals think that these third-party organisations may also want to increase their profits by leveraging individuals' data. Psychological consequences are also linked to third-party organisations, as third-party organisations have the ability to access large amounts of personal information and, for example, perform big data analyses. Individuals are unsure of how big data could be used in the future and thus feel uneasy.

Resource-related consequences, especially direct financial and material losses, are also perceived to be related to criminals. Individuals named criminals also as the source of prosecution-related consequences because they might try to transfer the responsibility of their illegal activities to an individual. Individuals associated intelligence services primarily with psychological consequences, in particular with a state of constant surveillance that they find highly uncomfortable. In addition, individuals associate intelligence services with prosecution-related consequences, because these services can trace illegal activities and forward their findings to authorities. Individuals also referred to intelligence services as a source of physical consequences because they have the power to suppress people by exercising physical violence or imprisonment. Some focus group participants also associated freedom-related consequences with governmental agencies that might try to manipulate people's political views. However, the participants agreed that manipulation could only be achieved by regimes exercising censorship or by exercising control over service providers (which is outside the scope of this study as it is not a consequence of accessing personal information).

Table 11 illustrates which different actors individuals perceive to be a potential source of different adverse consequences. The table depicts all identified actors and classifies them along the type of interaction, which can be either actively shared or unauthorised access to personal information, for instance, actors collecting individuals' information surreptitiously or buying or stealing the information from other organisations.

This multifaceted perspective of consequences and actors shows that organisations are directly associated with only a few of the perceived adverse consequences of access to individuals' information. Also, although an individual's objective might be to exclusively share information with a given organisation, other actors have many ways to gain access to personal information from interaction between the individual and the organisation. While an organisation is mainly interested in gathering and analysing customer data to provide and improve its services (and consequently increases its profits), its customers might be reluctant to share this information. In addition to the potential adverse consequences associated with the organisation itself, people can also fear consequences associated with external actors who might intercept, track, or otherwise gain access to their information. The question is to what extent an organisation both wants and needs to moderate the perceived consequences that individuals anticipate. These perceived consequences are not limited to those directly associated with the organisation itself, but include those that may arise indirectly out of this interaction. We thus examine how different actors can mitigate the perceived adverse consequences through behaviour, technology, and regulation.

We distinguish between preventive and corrective mechanisms, which influence perceptions of adverse consequences differently. Individuals and organisations can establish preventive mechanisms to restrict either

Table 11 Perceived adverse consequences of access to individuals' information and their associated sources

Type of interaction (between individual and actors)	**Actors** (potential sources of consequences)	**Perceived adverse consequences** (that arise from access to personal information and may affect an individual)						
		Physical consequences	Social consequences	Resource-related consequences	Psychological consequences	Prosecution-related consequences	Career-related consequences	Freedom-related consequences
Actively shared access Unintended access	Organisation (service provider)	☐	☐	☑	☑	☐	☐	☑
	Private contacts	☑	☑	☐	☑	☐	☐	☐
	Professional contacts	☐	☑	☐	☐	☐	☑	☐
Unintended access only	Third party organisations	☐	☐	☑	☑	☐	☐	☑
	Criminals	☑	☐	☑	☐	☑	☐	☐
	Intelligence services	☑	☐	☐	☑	☑	☐	☐

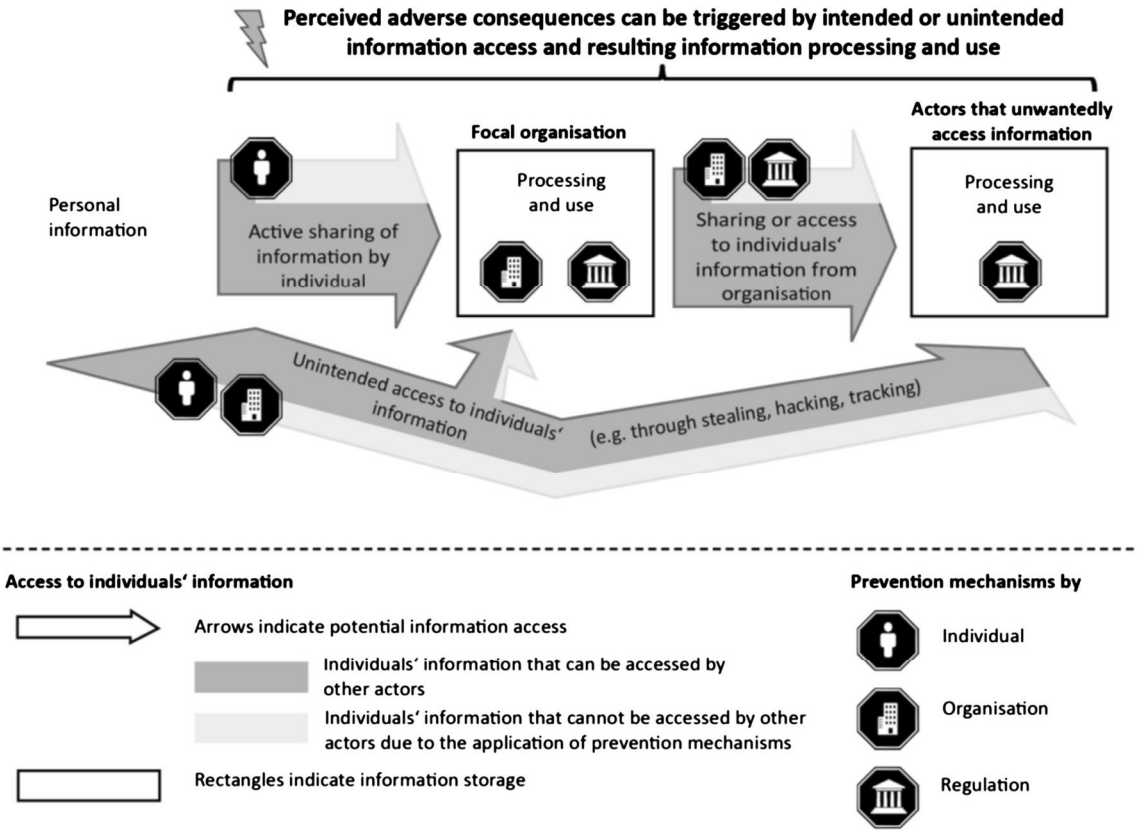


Figure 1 Information access and preventive mechanisms that may be used to restrict information access or use.

information access or information processing and use through behavioural and technical solutions and, in the case of public authorities, through regulation (see Figure 1).

If preventive mechanisms cannot be applied, are too expensive, or fail, then corrective mechanisms may be needed. Corrective mechanisms are used to reduce or eliminate the impact of a consequence. While a consequence may still occur, it has a lesser effect on the individual. In the following, we will discuss the different types of preventive and corrective mechanisms.

First, individuals see themselves as responsible for protecting their own privacy. Unfortunately, behavioural options for protecting one's privacy are rather limited once personal information has been revealed. Therefore, a person's activities mainly focus on preventing information disclosure if potential adverse consequences are perceived as being too severe. A first step is to decide not to share specific information. When deciding what information to disclose, people consider the adverse consequences they perceive may occur:

> I never uploaded any photos [on Facebook] which make me look bad or on which I'm totally drunk. Not even a photo on which I have a glass of alcohol in my hands. […] You often hear that your employers may find something like that and I am really afraid of that because I also want to have a decent job in the future (P6, FG3).

In addition to not actively sharing information, individuals focus on preventing access to their devices, for example by applying security-enhancing tools such as antivirus software and engaging in behaviours such as changing passwords regularly, deleting cookies, or using private browsing:

> Just recently I used a Microsoft tablet of a good friend and logged into an account. I did not select that my password should be saved or anything. Yet, when he used it the next day, I was still signed on with my Google account and he could see my calendar and other stuff. That was totally uncool. […] But for me, it wasn't obvious that I remain logged in. It can happen so easily. Now, I always do private browsing when I use devices of someone else (P3, FG8).

Again, we can see that individuals consider potential consequences when deciding about such activities. In general, those activities focus on preventing unauthorised access to specific data by preventing the tracking and stealing of data – not only by organisations but also by other external actors.

Once information is shared with or gathered by an organisation, the individual loses some control over this information. This may lead to further fears about potential adverse consequences, and people expect organisations to mitigate them. Organisational preventive mitigation mechanisms can take different forms. With internal secondary use of information as well as customer data that are actively transmitted, organisations can control actual consequences, for instance by changing organisational practices. However, organisations must deal with perceptions of consequences as much as with actual experiences, as customers' fears may be unjustified but nevertheless influence their decision-making. Increased transparency may be an effective strategy for easing customers' fears, and companies could go beyond the customary "privacy terms and conditions" by telling customers exactly how and why collected information is used, as well as what it is not used for. One focus group participant highlighted this possibility:

> Basically, I think it's a good thing if a company transparently communicates what happens with my data. That's how it should be. What happens in reality is a different thing, but I want to know the general plan, how it should be (P5, FG15).

To provide such a detailed statement, an organisation needs to analyse which perceptions of adverse consequences its customers have, so that it can then precisely target its communication to reduce the specific fears.

Furthermore, companies can grant users control over the settings of their customer profile. Managing specific pieces of sensitive information that are collected and stored, as well as controlling access to this information (e.g. private contacts or third-party firms), could decrease individuals' perceptions of certain adverse consequences. Companies could also partner with other service providers who are already trusted by the customers:

> I would say I'm really careful, but often you have to disclose information. If you want to buy something, then your bank account information is needed. However, what I normally do, I solely use PayPal. If I can't do a transaction via PayPal, if I have to directly disclose my bank account information, I just don't buy anything. I then prefer to do without that product (P1, FG18).

Reducing the possibility of adverse consequences from activities of other actors is also crucial in ensuring that those perceived consequences do not discourage customers from using an organisation's services. Nevertheless, this can be challenging, as organisations rarely have direct control over these outside actors. Most often organisations can only try to institute preventive mechanisms that either restrict or at the very least reduce the amount of information available to these actors. The focus group participants mentioned that internal data protection guidelines and security mechanisms should be in place and that organisations should also clearly communicate that they are. Like the transparency mechanisms discussed above, such strategies can effectively reduce customers' fears of adverse consequences:

> Yes, the security systems [of the organisation] have to be more secure, it should not be easy to hack them (P4, FG13), and Firms such as Facebook and Google that only make their money with customer data should thus spend huge amounts of money on [the security of] their servers (P2, FG13).

Yet, organisations cannot have preventive mitigation mechanisms in place for all types of consequences that

may result from the interaction of individuals with organisations. In some cases, only governmental regulations and laws, such as those related to data tracking and data storage, can act as mitigation of psychological fears. One participant, for example, talked about being filmed for Google Street View and how this potential privacy violation can only be addressed by governmental regulations:

> That's not an organisational issue. […] as a consumer I can't follow state-of-the-art technology, but I expect that I pay a certain amount of taxes and a higher authority is dealing with that for me […] which has the know-how, the access rights, and also can act executively. I think this cannot be addressed otherwise (P4, FG12).

Many of our focus group participants said they feel relatively secure because they live in a democratic, constitutional state that acts in the best interests of its citizens. They believe the government itself would not make use of personal information to suppress its citizens or undermine democratic values, at least at the current time:

> It is a big question which data secret services gather about us, we just do not know very much about this. (P4, FG17) That is exactly my concern. Everyone has a history and someone knows exactly what you have done at which point in time. Right now, it is irrelevant in our current social system and our democracy. Yet, you don't know what the world will be like in 30 years and whether someone may harm me based on what I have done in my past (P2, FG17).

Organisations can also institute corrective mechanisms that can help individuals to recover from actual consequences, should prevention prove to be impossible, too expensive, or ineffective. These mechanisms can reduce or eliminate the impact of consequences. One example of a corrective mechanism is compensation in the case of a financial loss:

> In my opinion […] people might make mistakes on the Internet and should be made responsible for those. Yet, if it is not their fault, then the organisations in whom I trust and to whom I gave my data, they have to compensate for the losses (P3, FG13).

As corrective mechanisms can only work if an adverse consequence of information disclosure can be reversed, they are particularly relevant in mitigating financial and material losses. Notably, however, the impact of all other consequences (e.g. social and physical) is most often irreversible.

In summary, as organisations are interested in their customers' data and perceived risks are a major factor in customers' decision to interact with an organisation, it is in the organisations' interest to mitigate customers' perceptions of adverse consequences. Organisations can use a range of behavioural and technical mechanisms to address customers' fears. These mechanisms need to be carefully adjusted to the specific consequences that the customers fear in particular situations. Implementing preventive or corrective mechanisms may not be sufficient if individuals are not fully aware of these mechanisms; effective communication of these mechanisms is needed. Nevertheless, organisations must be aware that their scope of influence may be limited, as some perceptions of adverse consequences cannot be addressed by the focal organisation. The great variety of actors involved increases that complexity further.

Discussion and implications

The results of our study indicate that individuals perceive a series of adverse consequences when their information is accessed by others. On the basis of our interpretive focus group study, we identified seven categories of consequences that individuals fear: social, physical, resource-related, psychological, career-related, prosecution-related, and freedom-related consequences. The first four categories (social, physical, resource-related and psychological) are in line with earlier risk studies in psychology and consumer research (Mitchell & Greatorex, 1993; Featherman & Pavlou, 2003; Luo *et al*, 2010). The novel finding of our privacy-specific investigation is the identification of the three remaining categories, namely career-related, prosecution-related, and freedom-related consequences. This finding indicates that access to individuals' information can trigger different risks than other events (Jacoby & Kaplan, 1972; Dowling, 1986; Mitchell, 1999) and that perceived consequences of these risks are manifold and far reaching. Building on these findings, we examined the sources that individuals identify for each of those consequences. Previous research has mostly focused on the direct interaction partners to which individuals disclose information (Krasnova *et al*, 2009; Anderson & Agarwal, 2011) and focused in depth on selected actors such as criminals (Jeong *et al*, 2012) or other third parties (Conger *et al*, 2013). Our results imply a richer network of attributions between perceived consequences and organisations (service providers), private and professional contacts, third-party organisations, criminals, and intelligence services. The different types of perceived consequences and associated actors allow the development of mitigation mechanisms that either reduce the perceived likelihood of a possible consequence of information access or mitigate its severity for the individual. Instead of looking at organisations' needs and priorities for privacy management (Greenaway & Chan, 2013), we turn the focus on individuals' perceptions that determine interactions with the organisation. The specific consequences that we identified allow privacy management to be used to modify individuals' perceptions of consequences by implementing mitigation mechanisms. The results and their implications for theory and practice will be discussed in more detail in the following.

Implications for theory

On the basis of our theorising on privacy, perceived consequences triggered by information access and our empirical study, we can derive the following implications and contribution to theory.

Perceived adverse consequences of information access The key limitation of extant literature focusing on individuals' perceptions about information collection and misuse and conceptualisation of privacy risks as an expectation of general losses (Malhotra *et al*, 2004; Xu *et al*, 2011; Smith *et al*, 2011; Dinev *et al*, 2013) is that possible consequences of information access are not addressed from an individual's perspective. Multiple facets of adverse consequences have been distinguished in other contexts (Featherman & Pavlou, 2003; Glover & Benbasat, 2010; Luo *et al*, 2010) and have been shown to be significant in areas such as consumer behaviour and psychology (Meichenbaum, 1977; Lazarus & Folkman, 1984; Featherman & Pavlou, 2003; Luo *et al*, 2010). At the same time, the comprehension of whether those facets apply to privacy and the existence of privacy-specific perceived adverse consequences has been limited. Our conceptualisation and categorisation of a wide range of perceived adverse consequences of access to individuals' information complements existing perspectives on information privacy by a consequence-oriented view that uncovers the actual reasons for individuals' fears and hesitations. From our focus group data we identified seven categories of consequences, of which three have not been conceptualised in other contexts, and several manifestations of each category. These manifestations contribute a deeper, privacy-specific understanding of the newly identified consequences, as well as of the existing consequences for which we develop richer multi-dimensional conceptualisations. Our theorisation on privacy-related perceptions of adverse consequences of information access addresses the calls for more research on privacy-related constructs that lie outside the traditional concept of privacy concerns (Bélanger & Crossler, 2011; Preibusch, 2013; Dinev, 2014).

Attributions of perceived adverse consequences Prior investigations have focused mainly on how and why different actors may gain access to personal information (Conger *et al*, 2013). We advance this body of knowledge by linking the actors which individuals perceive as a source to the specific consequences. Such in-depth mapping offers a differentiated view of the fears of individuals and takes into account how they relate to direct interaction partners as well as to other actors with potential access to personal information, specifically professional contacts, third-party organisations, intelligence services, and criminals. Even though the focal organisations might be the source of only a small number of adverse consequences, it is in their interest to mitigate all types of perceived consequences, as these might otherwise hinder consumers' future interactions.

Mitigation mechanisms and the role of organisations Prior literature has focused on how offering beneficial services can help to lessen privacy fears (Krasnova *et al*, 2010; Posey *et al*, 2010; Jiang *et al*, 2013) or how displaying seals or privacy notices may reduce fears of data collection and misuse (Hui *et al*, 2007; Tsai *et al*, 2011; Kim *et al*, 2016). We build on these studies by elaborating on how our categorisation and conceptualisation of perceived adverse consequences can inform the development and adaptation of mitigation strategies. Our differentiated conceptualisation of consequences and associated actors allowed us to theorise on two basic types of mechanisms that can be used to reduce individuals' fears: preventive and corrective mechanisms. Preventive mechanisms can alleviate fears by restricting information access or use that may trigger certain adverse consequences. Since organisations do not have full control over all data-related activities, they must send strong signals about their willingness to apply effective corrective actions when preventive mechanisms cannot be applied or fail. Thereby, individuals' concerns about sharing information can possibly be mitigated.

Our analysis also revealed that the scope of organisational influence is limited. For instance, sensitive data can be hacked and, depending on the type of data, financial compensation may not mitigate the consequences. Individuals then have to cope by themselves or rely on regulatory support for protection from negative consequences. Individuals can apply behavioural or technological measures as coping mechanisms if they are aware of potential information access, and laws and regulations are hoped to restrict an outside actor's illegitimate behaviour. Then again, given that organisations' intentional violations of individuals' privacy to obtain benefits cannot be fully prevented (Wall *et al*, 2016), perceptions of adverse consequences may remain even if mitigation mechanisms are applied.

Implications for practice

Firms often seek to collect as much information about their current and prospective customers as possible in order to tailor their services, increase their services' usefulness, and create stronger ties with their customers. They must monitor how this information gathering is perceived by their customers and which other actors influence customers' evaluation of the organisations' practises. We showed that while organisations are one of six sources of possible adverse consequences of access to individuals' information, also adverse consequences for which organisations are not directly responsible could considerably impede their business transactions. Hence, organisations should first determine which consequences their customers perceive may occur in specific transactions with them and are consequently of relevance to the organisation. Our overview of a range of possible consequences and how they map to specific parties can support this task.

We also identified several potential mitigation mechanisms that organisations can apply. The organisations' evaluation of which parties and associated adverse consequences are of primary concern for their customers should be followed by assessment of the feasibility, usefulness, and profitability of suitable mitigation

mechanisms. Our list of identified mechanisms can serve as a starting point for this assessment. Moreover, we want to highlight the importance of reducing individuals' *perceptions* of adverse consequences, as (1) the perceptions do not necessarily coincide with the actual consequences that might occur, and (2) organisations need to prioritise communicating their implemented mechanisms to their customers, or perceptions will remain unchanged. For example, enhanced security mechanisms might reduce the occurrence of actual negative consequences, but will not reduce the perceived adverse consequences if customers remain unaware of them.

Last, our results also provide important implications for policymakers, as certain consequences can only be mitigated through the establishment and enforcement of laws and regulations. However, policymakers must balance the interests of citizens with opportunities for attracting organisations and fostering innovative information-driven business models.

Limitations and suggestions for future research

Our study has some limitations and offers various opportunities for future research. We chose the focus group method to collect in-depth insights into individuals' perceptions and fears. While dynamic group interactions can foster the exchange of participants' thoughts and anecdotes and can sharpen the reasoning individuals provide when asked to contrast their own views to others' views, focus groups have several potential weaknesses. These include the risk that participants may be reluctant to speak openly in a group setting and the tendency towards convergent thinking. We tried to prevent these potential drawbacks by ensuring within-group homogeneity, conducting a large number of heterogeneous focus groups for theoretical saturation, and using well-trained focus group moderators (Fern, 2001).

Another limitation is that our sample came solely from the German population, possibly introducing a cultural bias. However, as Germans are particularly privacy-sensitive compared to other populations (EMC, 2016), we deemed this population to be especially useful for comprehensively collecting all potential adverse consequences. Future studies aimed at quantifying privacy-related risks in specific situations should carefully consider cultural influences in addition to context-specific influences.

Although our focus group data do not allow drawing conclusions about individual differences, our data indicate that individuals differ in their perception of the adverse consequences of access to individuals' information. Future research should extend our findings by using complementary methods such as surveys or experiments to uncover what drives these perceptions, individuals' estimated likelihood of those consequences in various situations, and why people differ in their perception of the degree to which different types of consequences are harmful and likely to occur. Accordingly, possible future research avenues include the impact of personality and situational cues on the perception of adverse consequences. Prior research has used surveys to understand the impact of personality traits on privacy concerns (Junglas *et al*, 2008) and could guide the design of such studies. An experimental design could be used to compare different situations and how situational cues might affect those consequences.

Lastly, more research is needed on the efficiency and effectiveness of preventive and corrective mechanisms. While methods such as security mechanisms, privacy policies, or seals have received attention in earlier research (Faja & Trimi, 2006; Hann *et al*, 2007; Hui *et al*, 2007; Kim & Kim, 2011; Mothersbaugh *et al*, 2012; Oetzel & Spiekermann, 2014), experimental studies could provide deeper understanding of how these mechanisms work and how they can be effectively designed.

Acknowledgements

We thank the editors and three anonymous reviewers for their feedback and guidance throughout the review process. In addition, we are grateful to Lisa Heller and our other student research assistants Katja Englberger, Viktoria Schlichte, and Christin Schaller for their support of this research project.

About the Authors

Sabrina Karwatzki is Research Assistant and Ph.D. Candidate at the Faculty of Business and Economics of University of Augsburg (Germany). She holds a M.Sc. in business informatics from the University of Mannheim, Germany. Her research focuses on the impact of information privacy on individuals and organisations. Her work appeared in journals including the *Journal of Management Information Systems* and the *Journal of Business Economics* and in conference proceedings, such as ECIS, HICSS, and AMICS.

Manuel Trenz is Assistant Professor at the Faculty of Business and Economics of University of Augsburg (Germany) and Research Associate in the Research Department for Information and Communication Technologies of the Centre for European Economic Research. He holds a Ph.D. from the Business School of the University of Mannheim, Germany. His research focuses on the implications of IT innovations on individuals' perceptions and behavior, including innovative digital services, channel convergence in retailing, and social issues arising in the areas of privacy or the sharing economy. His work has been published in *Journal of Management Information Systems*, *Business & Information Systems Engineering*, and in conferences such as ICIS, ECIS and AMCIS.

Virpi Kristiina Tuunainen is Professor of IS at the Department of Information and Service Economy of Aalto University School of Business (Finland). Her research focuses on ICT enabled or enhanced services and customer and community digital innovation. Her work has appeared in journals, such as, *MIS Quarterly*, *European Journal of Information Systems*, *Communications of the ACM*, *Journal of Management Information Systems*, *Journal of Strategic Information Systems*, *Information & Management* and *Information Society*; and in conferences, such as, ICIS, ECIS and HICSS.

Daniel Veit is Professor of Information Systems and Management at the Faculty of Business and Economics of University of Augsburg (Germany). He holds a master's degree in Mathematics from University of Giessen and a Doctoral degree in Business Economics from Karlsruhe Institute of Technology. His research focuses on market mechanisms, sustainability related topics as well as business model and entrepreneurial concepts in and beyond Information Systems including questions regarding multichannel commerce, privacy, digital healthcare and sharing economy. His work appeared in international journals and conferences amongst others the *Journal of Management Information Systems*, *Journal of Service Research*, *Business & Information Systems Engineering* and the *European Journal of Operational Research* as well as the proceedings of the ICIS, ECIS, AMCIS, HICSS, AMA and INFORMS conference series.

References

Abbasi A, Sarker S and Chiang RH (2016) Big data research in information systems: toward an inclusive research agenda. *Journal of the Association for Information Systems* **17(2)**, i–xxxii.

Acquisti A, Brandimarte L and Loewenstein G (2015) Privacy and human behavior in the age of information. *Science* **347(6221)**, 509–514.

Altman I (1975) *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Brooks/Cole Publishing Company, Monterey, CA.

Anderson CL and Agarwal R (2011) The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research* **22(3)**, 469–490.

Barbour R (2008) *Doing Focus Groups*. Sage, London.

Bauer R (1960) Consumer behavior as risk taking. In *Dynamic Marketing for a Changing World*, pp 389–398, American Marketing Association, Chicago, IL.

BCG (2013) The value of our digital identity. https://www.bcgperspectives.com/content/articles/digital_economy_consumer_insight_value_of_our_digital_identity/. Accessed June 29, 2013.

Bélanger F (2012) Theorizing in information systems research using focus groups. *Australasian Journal of Information Systems* **17(2)**, 109–135.

Bélanger F and Crossler RE (2011) Privacy in the digital age: a review of information privacy research in information systems. *Management Information Systems Quarterly* **35(4)**, 1017–1042.

BITKOM (2015) Internetnutzer gehen pragmatisch mit Datenschutz um. https://www.bitkom.org/Presse/Presseinformation/Internetnutzer-gehen-pragmatisch-mit-Datenschutz-um.html. Accessed January 22, 2016.

Chen J, Ping W, Xu Y and Tan B (2009) Am I afraid of my peers? Understanding the antecedents of information privacy concerns in the online social context. In *Proceedings of the Thirtieth International Conference on Information Systems* (Chen H and Slaugther S, Eds), Association for Information Systems, Phoenix, AZ.

Chiu C-M, Wang ETG, Fang Y-H and Huang H-Y (2014) Understanding customers' repeat purchase intentions in b2c e-commerce: the roles of utilitarian value, hedonic value and perceived risk. *Information Systems Journal* **24(1)**, 85–114.

Conger S, Pratt JH and Loch KD (2013) Personal information privacy and emerging technologies. *Information Systems Journal* **23(5)**, 401–417.

Corbin J and Strauss A (2008) *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Sage, Newbury Park.

Corbin JM and Strauss A (1990) Grounded theory research: procedures, canons, and evaluative criteria. *Qualitative Sociology* **13(1)**, 3–21.

Cunningham SM (1967) The major dimensions of perceived risk. In *Risk Taking and Information Handling in Consumer Behavior* (Cox DF, Ed), pp 82–108, Harvard University Press, Boston, MA.

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

Dinev T and Hart P (2006) An extended privacy calculus model for e-commerce transactions. *Information Systems Research* **17(1)**, 61–80.

Dinev T, Xu H, Smith JH and Hart P (2013) Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems* **22(3)**, 295–316.

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

EMC (2016) EMC privacy index. http://www.emc.com/campaign/privacy-index/index.htm?pid=home-emcprivacyindex-120614. Accessed September 29, 2016.

Faja S and Trimi S (2006) Influence of the web vendor's interventions on privacy-related behaviors in e-commerce. *Communications of the Association for Information Systems* **17**, 2–68.

Featherman MS and Pavlou PA (2003) Predicting e-services adoption: a perceived risk facets perspective. *International Journal of Human-Computer Studies* **59(4)**, 451–474.

Fern EF (2001) *Advanced Focus Group Research*. Sage, London.

Glover S and Benbasat I (2010) A comprehensive model of perceived risk of e-commerce transactions. *International Journal of Electronic Commerce* **15(2)**, 47–78.

Greenaway KE and Chan YE (2013) Designing a customer information privacy program aligned with organizational priorities. *Management Information Systems Quarterly Executive* **12(3)**, 137–150.

Hann I-H, Hui K-L, Lee S-YT and Png IPL (2007) Overcoming online information privacy concerns: an information-processing theory approach. *Journal of Management Information Systems* **24(2)**, 13–42.

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

Hui K-L, Teo HH and Lee S-YT (2007) The value of privacy assurance: an exploratory field experiment. *MIS Quarterly* **31(1)**, 19–33.

Jacoby J and Kaplan LB (1972) The components of perceived risk. In *Proceedings of the Third Annual Conference of the Association for Consumer Research* (Venkatesan M, Ed), pp 382–393, Association for Consumer Research, Chicago, IL.

Jeong B-K, Zhao K and Khouja M (2012) Consumer piracy risk: conceptualization and measurement in music sharing. *International Journal of Electronic Commerce* **16(3)**, 89–118.

Jiang Z, Heng CS and Choi BC (2013) Privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research* **24(3)**, 579–595.

Junglas IA, Johnson NA and Spitzmüller C (2008) Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems* **17(4)**, 387–402.

Kim DJ, Yim M, Sugumaran V and Rao HR (2016) Web assurance seal services, trust and consumers' concerns: an investigation of e-commerce transaction intentions across two nations. *European Journal of Information Systems* **25(3)**, 252–273.

Kim K and Kim J (2011) Third-party privacy certification as an online advertising strategy: an investigation of the factors affecting the

relationship between third-party certification and initial trust. *Journal of Interactive Marketing* **25(3)**, 145–158.
Kitzinger J (1995) Qualitative research. Introducing focus groups. *BMJ: British Medical Journal* **311(7000)**, 299–302.
Krasnova H, Günther O, Spiekermann S and Koroleva K (2009) Privacy concerns and identity in online social networks. *Identity in the Information Society* **2(1)**, 39–63.
Krasnova H, Spiekermann S, Koroleva K and Hildebrand T (2010) Online social networks: why we disclose. *Journal of Information Technology* **25(2)**, 109–125.
Lazarus RS and Folkman S (1984) *Stress, Appraisal, and Coping*. Springer, New York, NY.
Lincoln YS and Guba EG (1985) *Naturalistic Inquiry*. Sage, Newbury Park, CA.
Luo X, Li H, Zhang J and Shim JP (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 NK, Kim SS and Agarwal J (2004) Internet users' information privacy concerns (iuipc): the construct, the scale, and a causal model. *Information Systems Research* **15(4)**, 336–355.
McKinsey & Company (2013) Perspectives on retail and consumer goods. http://www.mckinsey.com/client_service/retail/latest_thinking/perspectives_spring_2013. Accessed January 22, 2016.
Meichenbaum D (1977) *Cognitive-Behaviour Modification: An Integrative Approach*. Springer, New York, NY.
Miltgen CL and Peyrat-Guillard D (2014) Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems* **23(2)**, 103–125.
Mitchell V-W (1999) Consumer perceived risk: conceptualisations and models. *European Journal of Marketing* **33(1/2)**, 163–195.
Mitchell V-W and Greatorex M (1993) Risk perception and reduction in the purchase of consumer services. *Service Industries Journal* **13(4)**, 179–200.
Mothersbaugh DL, Foxx WK, Beatty SE and Wang S (2012) Disclosure antecedents in an online service context the role of sensitivity of information. *Journal of Service Research* **15(1)**, 76–98.
Oetzel MC and Spiekermann S (2014) A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information Systems* **23(2)**, 126–150.
Parks R, Xu H, Chu C-H and Lowry PB (2016) Examining the intended and unintended consequences of organisational privacy safeguards. *European Journal of Information Systems* **26(1)**, 37–65.
Petronio S (2002) *Boundaries of Privacy: Dialectics of Disclosure*. State University of New York Press, Albany, NY.
Posey C, Lowry PB, Roberts TL and Ellis TS (2010) Proposing the online community self-disclosure model: the case of working professionals in France and the U.K. who use online communities. *European Journal of Information Systems* **19(2)**, 181–195.
Preibusch S (2013) Guide to measuring privacy concern: review of survey and observational instruments. *International Journal of Human-Computer Studies* **71(12)**, 1133–1143.
Sánchez Abril P, Levin A and Del Riego A (2012) Blurred boundaries: social media privacy and the twenty-first-century employee. *American Business Law Journal* **49(1)**, 63–124.
Sarker S and Sarker S (2009) Exploring agility in distributed information systems development teams: an interpretive study in an offshoring context. *Information Systems Research* **20(3)**, 440–461.
Van Slyke C, Shim JT, Johnson R and Jiang J (2006) Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems* **7(6)**, 415–444.
Smith HJ, Dinev T and Xu H (2011) Information privacy research: an interdisciplinary review. *Management Information Systems Quarterly* **35(4)**, 989–1016.
Smith HJ, Milberg SJ and Burke SJ (1996) Information privacy: measuring individuals' concerns about organizational practices. *Management Information Systems Quarterly* **20(2)**, 167–196.
Stewart DW, Shamdasani PN and Rook DW (2007) *Focus Groups: Theory and Practice*. Sage, Newbury Park, CA.
Strong DM and Volkoff O (2010) Understanding organization – enterprise system fit: a path to theorizing the information technology artifact. *Management Information Systems Quarterly* **34(4)**, 731–756.
Symantec (2015) State of privacy report 2015. http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf. Accessed January 22, 2016.
TRUSTe (2013) 2013 TRUSTe US consumer confidence index. http://www.truste.com/us-consumer-confidence-index-2013/. Accessed August 7, 2013.
Tsai JY, Egelman S, Cranor L and Acquisti A (2011) The effect of online privacy information on purchasing behavior: an experimental study. *Information Systems Research* **22(2)**, 254–268.
Wall JD, Lowry PB and Barlow JB (2016) Organizational violations of externally governed privacy and security rules: explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems* **17(1)**, 39–76.
Walsham G (1995) Interpretive case studies in is research: nature and method. *European Journal of Information Systems* **4(2)**, 74–81.
Westin AF (1967) *Privacy and Freedom*. Atheneum Press, New York, NY.
Wu Y, Ryan S and Windsor J (2009) Influence of social context and affect on individuals' implementation of information security safeguards. In *Proceedings of the Thirtieth International Conference on Information Systems* (Chen H and Slaughter S, Eds), Association for Information Systems, Phoenix, AZ.
Xu H, Dinev T, Smith J and Hart P (2011) Information privacy concerns: linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems* **12(12)**, 798–824.
Xu H, Teo H-H, Tan BC and Agarwal R (2009) The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems* **26(3)**, 135–174.

Appendix A: Focus group set-up

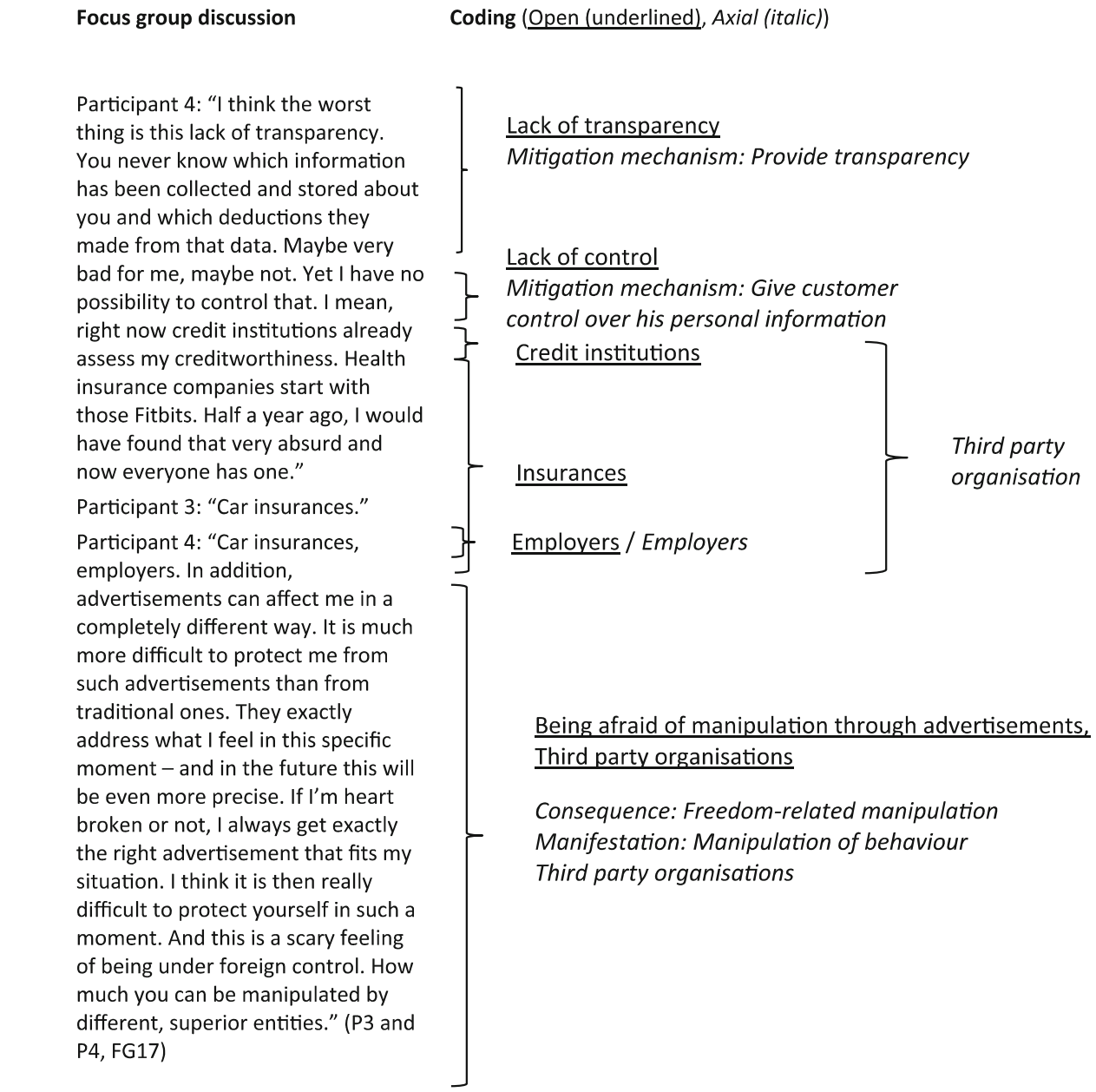
Focus group	*Composition*	*Age [average]*	*Number of participants [female/male]*	*Duration in min*
FG1	Pupils, 8th grade	13–14 [13.6]	6 [2/4]	40
FG2	Pupils, 10th grade	15–16 [15.5]	10 [7/3]	75
FG3	Pupils, 11th grade	17–18 [17.3]	8 [3/5]	90
FG4	Bachelor students	18–25 [20.6]	5 [2/3]	75
FG5	Bachelor and Master students	20–27 [23.0]	5 [1/4]	70
FG6	Bachelor and Master students	21–22 [21.6]	5 [5/0]	70
FG7	Bachelor students	21–23 [22.0]	5 [4/1]	60
FG8	Bachelor and Master students	22–24 [23.0]	4 [2/2]	70
FG9	Bachelor and Master students	21–25 [23.8]	5 [2/3]	100
FG10	Bachelor and Master students	21–25 [23.0]	5 [1/4]	100
FG11	Employees in a canteen	24–43 [31.0]	5 [3/2]	45

Focus group	*Composition*	*Age [average]*	*Number of participants [female/male]*	*Duration in min*
FG12	Calculation and aerospace engineers, management consultants, engineer in control and automation technology	24–58 [40.6]	5 [2/3]	90
FG13	Business engineer, insurance employee at the executive office of IT, sales representative, industrial clerk, sales representative	25–28 [26.0]	5 [2/3]	70
FG14	Head of marketing and product management, nurse, assistant office manager in a bank branch, employee in an engineering office, physiotherapist, architectural drafter	25–29 [26.5]	6 [3/3]	75
FG15	Factory mechanic, apprentice for health service clerk, educator, car body and vehicle builder, farmer	25–29 [27.0]	5 [2/3]	75
FG16	Truck driver, master craftsman in precision mechanics, industrial clerk, gardener, farmer	25–29 [27.8]	5 [3/2]	80
FG17	Journalists	28–68 [39.6]	5 [2/3]	95
FG18	Farmers, master electrician, agricultural engineer	38–51 [45.0]	4 [0/4]	40
FG19	Housewives and farmers	44–51 [47.6]	5 [5/0]	60
FG20	Tool set-up worker, employee at a publishing house, employees at a metal working company, teacher	45–62 [51.4]	5 [2/3]	65
FG21	Banker, police officer, group leader in quality assurance sector, lecturer in adult education, employee in an educational institute	50–58 [53.8]	5 [2/3]	105
FG22	Psychiatrists, psychoanalysts, psychotherapist, medical doctor	63–71 [65.2]	6 [2/4]	95

Appendix B: Interview guide for focus group conduction

1. Round of introductions
2. Activities and types of information that individuals perform/disclose online
   (a) Which online activities do you perform (e.g. usage of social networks, search engines, e-mails, online banking, online shopping, cloud services…)?
   (b) Which information do you share when performing these activities?
   (c) Which activities do you NOT perform online? Why not?
3. Information sensitivity
   (a) What is sensitive information? Why are these types of information sensitive?
4. Privacy concerns and privacy violations
   (a) Which concerns do you have when sharing personal information online (with respect to the activities that you do and don't perform)?
   (b) How could this information be misused? Who would be interested in using your disclosed information?
   (c) Which consequences could arise for you? Which losses do you associate with information disclosure?
   (d) Have you (or any person you know) ever been subject to a privacy violation?
   (e) Are there any activities that you perform, even though you see negative consequences that could arise? If yes, why?
   (f) Have you ever consciously changed your behaviour due to perceived risks?
5. Mitigation mechanisms
   (a) What do you do to actively manage your privacy?
   (b) Who is responsible for managing your privacy?
   (c) What do you expect organisations to do with respect to your privacy?

Appendix C: Excerpt coding



Appendix D: Evaluating trustworthiness (based on Lincoln and Guba (1985))

Evaluative criteria	*Goal*	*Appraisal*
Credibility	Assessment whether the results are believable	To ensure credibility, we followed the established guidelines by Fern (2001) on how to conduct focus groups. As we gathered data from 22 different focus groups, we gained a variety of insights from our 119 participants who varied in several dimensions such as age and experience as described above. Yet, in the end there was a lot of repetition of the different types of consequences being discussed in the focus groups so that we reached data saturation. Our focus group moderators were also well trained and thoughtfully guided the focus groups so that we are confident that our findings are congruent with perceived reality
Transferability	Assessment whether the results can be applied to other contexts	As the aim of our research is to provide a general categorisation of perceived adverse consequences that can arise when other parties have access to individuals' information, our findings are generally context-independent. These general findings enable context-specific research on perceived adverse consequences and enable future researchers to elaborate on those categories that are most relevant in their specific setting
Dependability	Assessment whether the findings are consistent	In line with Parks *et al* (2016), we ensured dependability by using inquiry audits: besides the authors themselves who assessed the process of focus group conduction as well as data coding and analysis, three colleagues at the authors' departments and four research assistants critically evaluated those steps, e.g. by scrutinising the interview guide and the identified concepts
Confirmability	Assessment whether the results are confirmable	All focus group transcripts were coded not only by the first author but also by an experienced research assistant to ensure that the findings accurately reflect the data. We also collected and integrated feedback from other researchers (professors and doctoral students outside our departments) that we received from various presentations and discussions

Appendix E: Empirical grounding of the study (based on Corbin and Strauss (2008))

Evaluative criteria	*What to look for in this study*
Criterion 1: Are concepts generated?	All presented concepts are grounded in the data. We derived them by conducting open and axial coding and constantly comparing and refining the evolving concepts. Exemplary quotes that illustrate our concepts are depicted in Tables 4, 5, 6, 7, 8, 9, 10 and "Appendix G"
Criterion 2: Are the concepts systematically related?	Our findings show how our concepts relate to each other. For example, we show that adverse consequences of access to individuals' information can be classified into seven categories. Moreover, we uncover further systematic relations by linking adverse consequences and the actors that may be seen as source of these consequences
Criterion 3: Are there many conceptual linkages and are the categories well developed? Do they have conceptual density?	We employed open and axial coding. Throughout these processes, concepts emerged were linked to each other and several early concepts were condensed into overarching categories. Thereby, we also ensured conceptual density of the categories by identifying and specifying the properties of all categories in detail
Criterion 4: Is much variation built into the theory?	Our study focuses on providing an extensive framework of all adverse consequences that may arise from access to individuals' information, associates the consequences with actors, and provides a discussion of the organisational scope of influence on mitigating those negative perceptions. Thus, our results are independent of a specific setting and serve as an overarching framework that can be contextualised in future studies that investigate information access in specific situations

Evaluative criteria	*What to look for in this study*
Criterion 5: Are the broader conditions that affect the study built into its explanation?	Although the aim of our study was to identify adverse consequences of information access independent of a specific context and to further analyse the role of actors in general, we expect that the importance of adverse consequences varies across contexts. In that sense, our framework facilitates a deeper understanding of how broader conditions impact adverse consequences
Criterion 6: Has process been taken into account?	This study identifies several mechanisms that can mitigate negative perceptions associated with access to individuals' information. We discuss conditions under which change may occur in section "Findings"
Criterion 7: Do the theoretical findings seem significant and to what extent?	As our findings are context-independent, we think that they can serve as a fundamental starting point for future research that aims at investigating context-specific privacy phenomena, in particular individuals' perception of situations where they fear an intrusion of privacy. We deem this as support of the significance of our findings
Criterion 8: Does the theory stand the test of time and become part of the discussions and ideas exchanged amongst relevant social and professional groups?	We are confident that our general framework of adverse consequences of access to individuals' information can inspire future research. In particular, we suggest conducting more contextualised studies which apply our findings to better understand individuals' privacy perceptions and behavioural reactions in specific circumstances. The identified framework of adverse consequences of access to individuals' information is comprehensive and should be stable over time; however, it is possible that the importance of different adverse consequences may change. Our types of adverse consequences allow a deeper investigation of such potentially salient evaluations

Appendix F: Research process evaluation criteria (based on Corbin and Strauss (2008))

Evaluative criteria	*What to look for in this study*
Criterion 1: How was the original sample selected? On what grounds?	We conducted 22 focus groups with 119 participants. We sought across-group heterogeneity and within-group homogeneity to collect insights from many different perspectives to ensure that no interesting findings are missed, while we preserved a homogeneous environment that fostered openness to sharing experiences that are as rich and detailed as possible
Criterion 2: What major categories emerged?	Seven categories of adverse consequences emerged: physical, social, resource-related, psychological, prosecution-related, career-related, and freedom-related consequences. Moreover, we identified six actors who can be the sources of those consequences and identified several mitigation mechanisms, which we also mapped to the different actors
Criterion 3: What were some of the events, incidents or actions (indicators) that pointed to some of these categories?	In each of the focus group sessions, the moderators encouraged the participants to share as many privacy-related experiences and incidents as possible and discussed each of them in depth. Transcripts of those stories, the perceptions of situations, and discussions amongst the participants were then coded and led to the categories and linkages reported in the "Findings" section and exemplified in Tables 4, 5, 6, 7, 8, 9, 10 and "Appendix G"
Criterion 4: On the basis of what categories did theoretical sampling proceed? That is, how did theoretical formulations guide some of the data collection? After the theoretical sampling was done, how representative did the categories prove to be?	Adverse consequences are the fundamental concept around which our study evolved. Thus, we followed an iterative process and gathered additional focus group data as long as new insights in terms of new consequences, new linkages to actors, or new mitigation mechanisms emerged. At the same time, we also ensured having a heterogeneous sample to not miss out important concepts. In the beginning, several of our concepts were very specific and fine-grained. Later, they collapsed into categories on a higher level of abstraction

Evaluative criteria	*What to look for in this study*
Criterion 5: What were some of the hypotheses pertaining to conceptual relations (i.e. among categories), and on what grounds were they formulated and validated?	Based on our data and an interpretation of them, we came up with hypotheses early on during data analysis. Examples of those hypotheses include that not only private contacts but also professional contacts can be the source of social consequences or that individuals see organisations as responsible for reducing other actors' access to personal information
Criterion 6: Were there instances in which hypotheses did not explain what was happening in the data? How were these discrepancies accounted for? Were hypotheses modified?	As the coding process continued, categories and linkages of those categories emerged. Several of these categories and related hypotheses held up, while others did not. For example, in the beginning, we had the impression that individuals mainly hold organisations responsible for mitigating the fears of adverse consequences. We eventually modified and refined this hypothesis as we discovered that several of the consequences are associated with other actors and cannot be controlled by organisations nor can their impact be mitigated by organisations
Criterion 7: How and why was the core category selected? Was this collection sudden or gradual, and was it difficult or easy? On what grounds were the final analytic decisions made?	Early on during the focus groups, when we investigated participants' privacy encounters, we discovered that they talked about concrete adverse consequences that they were afraid of rather than abstract concerns. We thus selected adverse consequences as the core category of our study. While other categories also emerged early on, all other concepts are linked to adverse consequences. This decision is grounded in our analysis and was validated with our focus group transcripts

Appendix G: Exemplary quotes for actors and associated consequences

Actor	*Adverse consequence of information access*	*Exemplary quote from focus group*
Organisation	Freedom-related	"Yes, as we said before with purchasing behaviour, so it is completely influenced and they first identify what interests me and thereby they make profits because then the advertisement shows up everywhere, it depicts of what I've already looked at or similar things that I might like. Of course I might see something then that I like and maybe I click on it. If they create those profiles of people, they also know what that person likes and that influences the purchasing behaviour for sure" (P6, FG3)
	Psychological	Participant 10: "Yes exactly, so, here on my cell phone I have, I used to have some kind of location-tracking protocol from Google. I turned that off now. I could see when I…I went on Google and then you could check where the phone was. So you could see exactly where you were walking, how long, how fast Participant 9: "How precise was that?" Participant 10: "It was precise up to 10 meters. Precise up to 10 meters! And on the map you could really see that, I don't know, I'm at the airport and I just passed the security check when I flew to China. And that was a little bit scary" (P9 and P10, FG2)
	Resource-related	Participant 2: "I just wanted to say, I do only use certain online shops. For example, I use Zalando, I buy stuff there, but I would not buy things at any smaller shops, sometimes you see these websites where the offer ideas for presents etc. I would never buy anything there" Moderator: "Why is that?" Participant 2: "I'm afraid that they'll either never get my money […] Or that they clear out my account" (P2, FG15)
Private contacts	Social	"It's the same thing in clubs. If you are responsible for young club members and there is some kind of picture, you boozing with young people, then immediately other club members or people of your village, because we live in a small village, say […] that's not good company for my child" (P2, FG 16)
	Physical	"Once it happened that I was threatened by someone via Facebook. I was really extremely glad that I hadn't shared any sensitive data online. I was really in panic because if my exact residence or my real name or other things like that had been available, it would be much easier to find me in a city not too big such as Munich" (P4, FG10)

Actor	*Adverse consequence of information access*	*Exemplary quote from focus group*
	Psychological	"For me it is also that I don't want everybody to know everything about my life at a glance. Because I think that today, if you tell somebody your name on Facebook, that person knows a lot, if you were tagged on pictures somehow and even though you didn't disclose a lot of information, but you still see the person has these friends, went to that school or lives in that town. So I think, you can get a lot of information that way. I don't want any additional information to be so easily accessible there" (P2, FG9)
Professional contacts	Career-related	"Regarding the whole job aspects – it's not my experience but that of a former colleague of mine – she was sick-listed for the whole week and at the weekend she went to a party where some picture were taken, which were then published on the webpage of a local newspaper. Our apprenticeship instructor saw it and she got a warning letter" (P4, FG5)
	Social	"I ran into difficulties with someone on a professional level and then I took the time and did research on the Internet what kind of a person he is or how his business is rated and a poor light was cast upon him. And then it took me a lot of time until I said, okay, now I'll invest a day and drive out there and meet him in person and by doing that I realised how much reality I had lost through the Internet. So when I perceive someone face-to-face and talk to that person and look them in the eyes and say, what is going on there and how the person reacts, that is a much greater range of information that I get and that is the danger I see that we rely more and more on information available on the Internet and take it for reality which actually isn't true" (P3, FG12)
Third-party organisations	Freedom-related	"That will be taken into greater account, especially with health insurance and things like that. If you, whatever, look up an illness several times on Google or check what it might be, it's possible that they can already retrace, something is going on with him. Then you want supplementary insurance, then they see that, the person already looked that up three times and then they already have concerns" (P3, FG18)
	Psychological	"As I said before, [I would be afraid] that someone has an extensive profile of me, with all my habits, what I buy every month and what I spend money on. I think that's nothing but my private business. It's not that I have anything to hide or do something criminal, it's just that third parties should not know what I spend my money on" (P2, FG8)
	Resource-related	"I see hazardous potential here. It'll probably be only accomplished in five to ten years, but then you'll be under constant surveillance, like happy cows, and someone will calculate our remaining life time and then adjust insurance policies to that. And everyone who does not want to be under surveillance will automatically be placed into a worse category, will be subliminally criminalised, with the assumption that he must have a good reason for acting like this. That's what I'm afraid of" (P3, FG12)
Criminals	Prosecution-related	"I don't know, if one registers at a pornographic website or any other illegal website or downloads something, a video, using my account, yes and then I have the problem. Then I might be reported to the police or something like that" (P4, FG6)
	Physical	Participant 2: "On social media by criminals, just by persons that deliberately want to harm somebody possibly using cyberbullying. Or also specifically by perpetrators who want to kill or waylay someone, who want to stalk. I would say there is a considerable risk because everybody can get access to the data without having to specifically hack into something or…" Moderator: "Do you mean things like your location or your address by that?" Participant 2: "For example or everything you post there, pictures with friends and so on. Because he can find out everything about your life and then of course do something bad" (P2 and Moderator, FG5)
	Resource-related	"Maybe I might also be afraid of somebody, who has a cost profile of me, knowing, oh she booked a vacation for this and that week, she won't be home then. Criminals might know that the place is vacant. One often doesn't know who's behind it. So that's what I would be afraid of" (P2, FG8)
Intelligence services	Prosecution-related	Participant 3: Besides the fact that I'm not a criminal, I would never go to pornographic webpages, they always appear to be so unsafe." Moderator: "What is unsafe?" Participant 3: "Pornographic webpages. All that stuff. I'm not interested in that, but I would never search for something like that, it's so dubious" Moderator: "Well, what could they do with your data?" Participant 3: "I would be afraid that the police is immediately at my front door, just because I click on such a webpage" (P3 and Moderator, FG16)

Actor	*Adverse consequence of information access*	*Exemplary quote from focus group*
	Physical	"If I think of drones being controlled by the Americans, they use your mobile phone, then [the misuse of your location data] may result in your death. […] Someone informs them about your name and says that you are a bastard. And then they use your mobile phone number and shoot this mobile phone" [P4, FG12)
	Psychological	Participant 2: "I personally know that I reveal personal information via Facebook and WhatsApp, but I accept the risks to stay in touch with my friends. Even if I still watch out, but I'm aware that I release data there" Participant 5: "Whereas, I assume that large organisations, actually intelligence services, pose the actual danger here because all of that data has to be analysed. So it can, I don't see the danger that some, let's say a hacker, some criminal can make use of it. That is only possible on a large scale" (P2 and P5, FG12)

Appendix H: Exemplary quotes for a comparison of consequences across age groups

To get an understanding of potential differences, we further analysed our data after the axial coding process.[1] As described in section "Research method", we conducted exploratory focus groups to get an overview of all possible perceptions about adverse consequences. In line with this research goal, all discussions were very broad and open and each focus group covered the topics regarding access to individuals' information that our participants experienced or were knowledgeable about. The discussions were based on situations and contexts that they usually engage in. Thus, counting individual occurrences does not do justice to the research method and might foster overinterpretation. Comparing occurrences numerically could even lead to wrong conclusions if certain types are excessively mentioned in one group but rarely mentioned in others groups, just because discussions in this group focused on different experiences. Yet, we were interested whether our data would give us an indication on potential differences between groups that could be further explored in future research. We therefore carefully reanalysed it to identify extreme differences between the groups. However, we did not find any noticeable differences with respect to age or background. Our analysis reveals that all categories of consequences were mentioned throughout all age groups and across backgrounds several times. The following table provides an exemplary illustration of this result by exhibiting one exemplary citation for each combination of category and age (Tables 12, 13, 14, 15, 16, 17, 18).

[1]We thank an anonymous reviewer for highlighting this possibility.

Table 12 Prosecution-related consequences

Age group	*Exemplary quote from focus group*
Students	"I don't know, but if someone registers at a porn website or elsewhere at an illegal website, or downloads something, a video, using my account then it's my problem. Then, there might be brought a charge against me or something like this." (P4, FG6)
Adults 25–35	Participant 4: "Or maybe that murder which was resolved. They solved it because they could track the mobile phone. Not right at the incident but rather two weeks after the incident they could look up where this guy was with his phone. It's nothing but my private business where I'm touring. Sure, in this case it's fine. But all of my steps are tracked as well, and that is something where I say…" Participant 6: "You only need to be in the wrong place at the wrong time." (P4 and P6, FG14)
Adults older than 35	Participant 4: "Okay, but there are countries, for example somewhere in the Ukraine there was the case that everyone got some SMS notifications based on their current location…" Participant 3: "A transmitting mast, they were logged onto." Participant 4: "…that they are participating in a demonstration, an illegal demonstration and that they all got registered. I mean that's quite concrete – sure that's the Ukraine and not us –, but we can't be sure that one day we'll be in the same situation." (P3 and P4, FG17)

Table 13 Social consequences

Age group	*Exemplary quote from focus group*
Students	"Recently on Facebook, I indicated that I might participate in an event which was named 'Dicht und Ergreifend' ('Dicht' has two meanings in German: dense and drunk; thus it's ambiguous whether the event is called 'Dense and Thrilling' or 'Drunk and Thrilling') and then one of my friends googled me – for another reason, because of a research project we worked on together. And the first result on Google was '[Participant 4] participated at 'Dicht und Ergreifend'. The event had not yet taken place, I just clicked 'maybe' on Facebook and this was the first result you found if you googled me. I will never ever participate in events [on Facebook] again. For sure, they laughed about me, but for me it was serious, it stated she participated at 'Dicht und Ergreifend'." (P4, FG7)
Adults 25–35	Moderator: "Okay, let's go back to the statement you made about the potential usage of your personal data. For instance, you said that someone may use them to create a fake profile on Facebook with your name and all of your information. Which losses do you associate with that?" Participant 1: "Societal calumny. Yes, that's one possibility. Loss of friends. Yes, it sounds primitive but it's true, loss of friends." Participant 3: "Yes, that is true." Participant 1: "Loss of other people's trust, including friends, family, if someone publishes something in your name, then no one will trust you anymore because they think you publish everything on Facebook. Even if you tell them twenty times it's not you." (M, P1, and P3, FG16)
Adults older than 35	Participant 2: "It's the same thing in clubs. If you are responsible for young club members and there is some kind of picture, you boozing with young people, then immediately other club members or people of your village, because we live in a small village, say that…" Participant 3: "Bad company for the youth." Participant 2: "No, that's not good company for my child." (P2 and P3, FG 16)

Table 14 Physical consequences

Age group	*Exemplary quote from focus group*
Students	"I think, partially you make yourself more vulnerable, for instance I heard about cases in which stalkers used things such as information you disclosed on the Internet. Then they know where you live and what you do all day, your habits and so on. That offers quite a good platform to identify individuals for people with those [stalking] tendencies." (P2, FG7)
Adults 25–35	Participant 4: "Any people that somehow – do not make fun of it – but you see it more and more often that especially men download something about women. I just find it scary that someday someone might go after me or something. Like on Facebook. He knows you, he knows where you live and for instance he could just follow you." Participant 1: "But stalkers already existed before the age of the Internet." Participant 3: "But now it is increasing." Participant 4: "Now it's stronger." Participant 3: "Now it's easier for them." Participant 1: "Now stalking is easier, yes that's true." (P1, P3, and P4, FG16).

Table 14 Continued

Age group	*Exemplary quote from focus group*
Adults older than 35	"When it comes to my kids I'm quite careful with respect to private issues. I won't share any pictures of her, but if you think about the possibility of pictures of my 13-year-old daughter on the Internet and of course the location history via her mobile phone or via Facebook, because she often shares her current location, then you can put all things together, how the person acts and that can be used to harm her at a certain time. That's quite disturbing me." (P4, FG13)

Table 15 Career-related consequences

Age group	*Exemplary quote from focus group*
Students	"Regarding the whole job aspects – it's not my experience but that of a former colleague of mine – she was sick-listed for the whole week and at the weekend she went to a party where some picture were taken, which were then published on the webpage of a local newspaper. Our apprenticeship instructor saw it and she got a warning letter." (P4, FG5)
Adults 25–35	Participant 2: "Well, once [a picture of you] is on the Internet, it'll be there forever. Now, imagine someone posts a picture of me where I'm totally wasted. If I am then looking for a new job, my employer may say, well, let's have a look at what this woman did recently. He may find that picture and that may result in me not being hired." Participant 1: "Just because you were drunk two years ago?" Participant 2: "Yes, well…." Participant 5: "Every employer who is hiring probably checks such things." (P1, P2, and P5, FG 7)
Adults older than 35	Participant 3: "Yes, loss of job. Or within an organisation, if you are involved in a brawl and got photographed while you are drunk, that goes viral in my organisation. That's not beneficial for my career." Participant 4: "Yes. That can result in problems regarding your promotion." Participant 3: "Yes, definitely." Participant 4: "Career interruption." Participant 3: "You'll need to justify that for sure." (P3 and P4, FG21)

Table 16 Freedom-related consequences

Age group	*Exemplary quote from focus group*
Students	"It is well known that advertisement appears that fits with things you just looked up. But how much can they manipulate me with all these data? How much of this do you even notice, and moreover you don't know how this is influencing your behaviour, whether you would have bought that anyways or only due to the advertising." (P5, FG2)
Adults 25–35	Participant 4: "I think the worst thing is this lack of transparency. You never know which information has been collected and stored about you and which deductions they made from that data. Maybe very bad for me, maybe not. Yet I have no possibility to control that. I mean, right now credit institutions already assess my creditworthiness. Health insurance companies start with those Fitbits. Half a year ago, I would have found that very absurd and now everyone has one." Participant 3: "Car insurances." Participant 4: "Car insurances, employers. In addition, advertisements can affect me in a completely different way. It is much more difficult to protect me from such advertisements than from traditional ones. They exactly address what I feel in this specific moment – and in the future this will be even more precise. If I'm heart broken or not, I always get exactly the right advertisement that fits my situation. I think it is then really difficult to protect yourself in such a moment. And this is a scary feeling of being under foreign control. How much you can be manipulated by different, superior entities." (P3 and P4, FG17)
Adults older than 35	"What is interesting to note is that you disclose information unintentionally, only by searching for things. What I notice is that when you look for particular products on Amazon, particular products are displayed to you in the near future, just… you disclose things without writing them down, just due to your behaviour [on the Internet]. And I get more and more aware that the user behaviour gets analysed and you receive preselected information that you need, and this is how you get externally controlled." (P2, FG18)

Table 17 Psychological consequences

Age group	*Exemplary quote from focus group*
Students	Participant 10: "I used to have kind of a location profile at Google on my mobile phone. In the meantime, I have deactivated it. When I looked it up on Google, you could see the location history of my mobile phone, really, where you went, how long, how fast." Participant 9: "How precise was it?" Participant 10: "It was precise up to 10 meters! Really, you could see on the map that, I don't know, I was at the airport and just passed the security control, as I flew to China. That was kind of frightening me." (P9 and P10, FG2)
Adults 25–35	"That's where I struggle. On the one hand it is so bad that they use your information. But on the other hand, I ask myself what evil things they should do with it. But… it's so difficult to grasp this. What do they aim at, it's so…" (P6, FG14)
Adults older than 35	"And because it is that way, sometimes this evokes a try… or the feeling of being monitored by others who know what you're doing, what you're buying, what you're selling, when you're selling it. I don't like this, it's irritating, but… in addition, with these modern cars, when I activate the navigation unit everyone knows where I am at any time." (P1, FG22)

Table 18 Resource-related consequences

Age group	*Exemplary quote from focus group*
Students	Participant 2: "I think, with respect to the location topic, it is dangerous too, when it comes to some imprudent posts, for example "now two weeks of vacation". It doesn't even have to be a criminal or a company but simply individuals who think: "I know where you live, I know that you are on vacation, why don't I just break in?" That already happened." Participant 3: "Right." Participant 2: "It's not necessarily organised crime, but there are individuals that make profit out of you posting such things imprudently." (P2 and P3, FG4)
Adults 25–35	Participant 1: "Well, I don't know if this is that serious, but if I shared where I am and they would know where I live, they could easily raid my place. It sounds stupid, but…" Participant 4: "But it is true." Participant 5: "That's undeniably the case." (P1, P4, and P5, FG11)
Adults older than 35	Participant 5: "For instance, I don't do online banking because I'm afraid of the misuse of my bank data." Participant 1: "Actually, I just pay with – what's the name again…" Participant 2: "PayPal." Participant 1: "PayPal, with PayPal and I use it seldom, only if I have no choice. If I need something from eBay and there is no other way and the amount of money is not high, I do it, but not with higher amounts of money. Up to 100€, that's the limit. For me, the risk is too high, despite of PayPal, notwithstanding their statement that you get your money refunded, for me it's not worth the stress." (P1, P2 and P5, FG20)