Electronic Markets (2022) 32:2333–2355
https://doi.org/10.1007/s12525-022-00522-6

RESEARCH PAPER

Perceived privacy risk in the Internet of Things: determinants, consequences, and contingencies in the case of connected cars

Nils Koester[1] · **Patrick Cichy**[2] · **David Antons**[1] · **Torsten Oliver Salge**[1]

Received: 5 February 2021 / Accepted: 4 January 2022 / Published online: 9 June 2022

Abstract

The Internet of Things (IoT) is permeating all areas of life. However, connected devices are associated with substantial risks to users' privacy, as they rely on the collection and exploitation of personal data. The case of connected cars demonstrates that these risks may be more profound in the IoT than in extant contexts, as both a user's informational and physical space are intruded. We leverage this unique setting to collect rich context-immersive interview (n = 33) and large-scale survey data (n = 791). Our work extends prior theory by providing a better understanding of the formation of users' privacy risk perceptions, the effect such perceptions have on users' willingness to share data, and how these relationships in turn are affected by inter-individual differences in individuals' regulatory focus, thinking style, and institutional trust.

Keywords Information privacy · Disclosure decision-making · Perceived privacy risk · Connected cars · Internet of Things

JEL classification O33

Introduction

Smart, connected devices range from fitness trackers to intelligent streetlights (Porter and Heppelmann 2014) and gradually permeate all areas of life (Lowry et al. 2017). Within this emerging Internet of Things (IoT), connected cars are a particularly relevant and consequential case. Equipped with ever more powerful sensors and actuators, connected cars not only collect a continuous stream of car-, driving- and context-related data, but also locate the car in the broader mobility network. Novel services that are enabled by car connectivity are meant to assist the driver in the actual driving activity and in associated tasks. For example, smart parking services help drivers to find and book vacant parking spots. Driving style analytics, as another example, help car users to drive more eco-friendly by providing them with real-time feedback. Augmenting the driving task in such ways promises to enhance the overall driving experience and comfort. However, to make use of such novel car functionalities and associated services, drivers need to cease control over various types of car data that might also contain information about their behavior and preferences (e.g., inferred from vehicle position, route, acceleration, speeding, infotainment). This diminishes drivers' information privacy (Stone et al. 1983; Westin 1967) and exposes them to new and far-reaching negative consequences that even include threats to their physical safety (Lowry et al. 2017).

At a broader level, the case of connected cars highlights new challenges that users of smart, connected devices generally face, as most of such devices are associated with privacy risks that needed to be evaluated in the course of the

Responsible Editor: Soheil Human

This paper is an extension of a paper presented at the HICSS 54 - Track "Human-centricity in a Sustainable Digital Economy"

✉ Nils Koester
nils.koester@time.rwth-aachen.de

Patrick Cichy
Patrick.Cichy@bfh.ch

David Antons
antons@time.rwth-aachen.de

Torsten Oliver Salge
salge@time.rwth-aachen.de

[1] RWTH Aachen University, Institute for Technology and Innovation Management, Kackertstr. 7, 52072 Aachen, Germany

[2] Bern University of Applied Sciences, Institute of Applied Data Science & Finance, Brueckenstr. 73, 3005 Bern, Switzerland

adoption decision. In that regard, connected cars shed light on some of the unique characteristics of the IoT – not least regarding the continuity of data collection, the lack of user control over data collection, the interdependence between data collection and device functionality, as well as devices' potential impact on users' informational and physical space (Cichy et al. 2021). Hence, the context of connected cars appears to be a particularly fertile ground to review and potentially extend current research on users' privacy risk perceptions and their data sharing decisions. Deeply embedded in the connected car context, our study draws on both interview data from 33 participants and survey data from 791 German car drivers to contribute to extant research on users' formation of privacy risks (Malhotra et al. 2004) and the adoption of privacy-invasive information systems (IS) (Dinev and Hart 2004).

First, we use our context-immersive interview data to dive deep into the connected car context and unearth the specific risks that car drivers associate with the use of a connected car and the collection of their car data. Building on prior studies on perceived (privacy) risk in consumer decision making (e.g., Dowling 1986; Glover and Benbasat 2010; Karwatzki et al. 2018), we develop a rich inventory of privacy risks that reflects the broad set of potential negative consequences associated with the loss of control over car data. These consequences can be clustered into *psychological* (e.g., feelings of surveillance), *physical* (e.g., vehicle manipulation by hackers), *social* (e.g., stigmatization as a poor driver), *financial* (e.g., increased car insurance cost), *freedom-related* (e.g., unsolicited ads), *prosecution-related* (e.g., identification of traffic offenses), and *career-related* (e.g., evaluation during driving jobs) threats. The inventory illustrates not only the multidimensional nature of data-related risks in the IoT, but also the blurring of the formerly-distinct concepts of information privacy and physical privacy (Smith et al. 2011). Importantly, this inventory also serves as the basis for the development of a novel 15-item measurement instrument for users' car-data-related risks. This measure captures the specific nature of negative consequences users associate with a loss of control over their car data. Importantly, this measure is conceptually and empirically distinct from, yet predictive of, the more general construct of perceived privacy risk, which has been criticized for being too ambiguous (Li 2012) and too abstract (Karwatzki et al. 2018). Our results suggest that context-independent and context-specific privacy measures can complement instead of substitute each other when it comes to explaining the formation of privacy risk perceptions and data sharing decisions. We believe that our risk inventory and the associated measurement instrument can be of broader appeal for contextualized theorizing (Hong et al. 2014) and significantly advances the understanding of privacy as an contextual concept.

Second, we leverage the unique properties of our connected car setting and our large-scale survey data from 791 car drivers to better understand how users differ in their formation of privacy risk and the extent to which these beliefs impact their willingness to share data. Identifying and explaining such potential differences between users is conceptually and practically relevant, in that it increases the explanatory power of extant privacy models and offers a novel starting point for user segmentation (Dinev et al. 2015). We build on extant research on the role of trust in disclosure decision-making (e.g., Dinev and Hart 2006) and find car drivers that trust the data-soliciting car manufacturer to be more inclined to share their car data in presence of perceived privacy risks than those that do not. With this we add to the growing literature stream that incorporates ideas from cognitive psychology to enhance models of individual privacy risk formation and data sharing (Dinev et al. 2015). More specifically, we draw on regulatory focus theory (Higgins 1998) and interpersonal differences in *prevention focus* (i.e., individuals being primarily motivated by avoiding negative outcomes and losses). We argue that car-data-related risks will translate more strongly into perceived privacy risk when drivers exhibit a strong rather than a weak chronic, i.e., habitual, prevention focus and a disposition toward avoiding losses. Even though we fail to find empirical support for such a moderating effect, we find evidence for a substantial negative direct effect of prevention focus on perceived privacy risk. In regard to individuals' thinking styles (Epstein et al. 1996), we find that perceived privacy risks will translate more strongly into low levels of willingness to share car data among drivers with a high rather than a low need for cognition, that is an inclination toward deep reflection and high cognitive elaboration rather than heuristic decision-making. With this, our study contributes to a richer understanding of individual-level contingency factors in view of developing privacy models with high explanatory power in the connected car context and arguably IoT more broadly. Next, we present the conceptual background and our hypotheses.

Theoretical background

Privacy risks and disclosure decision making

Consumers must anticipate various risks in their daily decisions. Their perception of risks is said to be a function of possible negative consequences of each choice and the likelihood of their occurrence (Dowling 1986). Perceived risks significantly influence, for example, whether consumers adopt certain service offerings (Glover and Benbasat 2010) or how satisfied they are with such (Keh and Sun 2008). In today's digitized society, significant risks for consumers

arise from the fact that their personal information is being systematically collected, stored, and analyzed (Malhotra et al. 2004), be it for the sake of marketing activities, to personalize service offerings, or to create novel data products.

Conceptualizations of privacy risk aim at capturing an individual's expectations of the consequences of privacy-invasive practices for them. Here, two streams can be identified. First, some studies define privacy risk as an individual's belief that parties will behave opportunistically if they receive access to personal information (Dinev and Hart 2006). Second, other studies conceptualize privacy risk as an individual's expectations of potential disadvantages or unexpected problems associated with data disclosures (e.g., Dinev et al. 2013; Malhotra et al. 2004). A somewhat related conceptualization in the realm of privacy-related risk beliefs are privacy concerns (Smith et al. 2011). Associated measurement instruments are meant to reflect individuals' concerns about how organizations handle their personal data. The widely used *Concern For Information Privacy scale* (CFIP; Smith et al. 1996), for example, captures how much individuals bother in general about a potential collection, secondary use, errors, and unauthorized access of their personal data (Smith et al. 1996).

The anticipation of privacy risk has frequently been shown to reduce individuals' intention to share personal data, respectively to adopt privacy-invasive products and services (e.g., Kehr et al. 2015; Smith et al. 1996). In fact, privacy risk is depicted as the most influential factor in such consumer decisions (e.g., Malhotra et al. 2004). The role of the privacy-related risk beliefs in consumer decisions has been the focus of studies in various contexts, like online shopping, healthcare or social online networks (e.g., Jozani et al. 2020; Malhotra et al., 2004; Krasnova et al. 2010; Trepte et al. 2020) (see Appendix 20 for a literature review). However, scholars have only recently begun to explore the formation and behavioral consequences of perceived privacy risk in IoT-related contexts.

Privacy risks in the context of connected cars

Lowry et al. (2017) argues that smart and internet-connected devices associated with the IoT pose novel privacy challenges that expand beyond what we have experienced in other contexts. This is due to the novel streams of data they emit as well as to the consequences resulting from their cyber-physical nature. The latter entails that data-related risks can also pertain to one's physical safety (Cichy et al. 2021). Connected cars are a particularly interesting case in that regard, as they generate large amounts of highly specific data allowing inferences on car health, driving behavior, road conditions, and routes traveled. In the highly regulated context, this data can not only reveal, for example, inappropriate handling of the vehicle and violations of traffic rules. Improper access and manipulation of such data can also entail the malfunctioning of vehicle functionalities (Lowry et al. 2017). As an example, incorrect information on road obstacles may trigger inadequate emergency braking and a potential collision.

Against the novelties introduced by connected cars, we believe that a context-sensitive research approach is needed to fully understand perceptions and consequences of privacy risk. Several scholars have long advocated the idea to pay close attention to the idiosyncrasies and usage context of the IS artifact in order to arrive at robust recommendations for IS design and practice (Orlikowski & Iacono, 2001). In line with these calls, we follow recommendations put forward by Hong et al. (2014) in developing and testing a conceptual model explaining car data disclosure decisions. Our approach is twofold. First, we expand extant theory on data disclosure decisions by considering the effect of individuals' level of chronic prevention focus, need for cognition, and trust towards the car manufacturer (level 1 contextualization). Second, we contextualize existing (e.g., perceived privacy risk) and create a complementary, entirely new measurement instrument (i.e., car-data-related risks) to being able to capture the specificities related to connected cars (level 2b contextualization). In the same vein, we identify various control variables that are of particular relevance for data disclosure decisions in the context of connected cars. Figure 1 shows the contextualized research model, which we develop in the following section.

Hypotheses

Determinants of perceived privacy risk

According to the general theory of perceived risk (Dowling 1986) and insights on privacy-related risks in particular (Karwatzki et al. 2018), we argue that individuals' perception of privacy risk relies on their evaluation of potential negative consequences that arise from others having access to ones' personal data. In forming risk beliefs, individuals evaluate negative consequences regarding how far-reaching as well as to how likely they are. Negative consequences that are specific to the disclosure of personal data have been categorized into several dimensions such as physical safety, social status, and freedom-related risks (Karwatzki et al. 2017). While these might hold across various settings in which privacy invasions take place, the exact manifestations of negative consequences are closely tight to the specific context and rely on factors such as involved data types, usage context, or stakeholders (Smith et al. 2011). Scholars revealed that individuals associate various types of negative consequences with data disclosure in the context of connected cars and argued that these might explain the

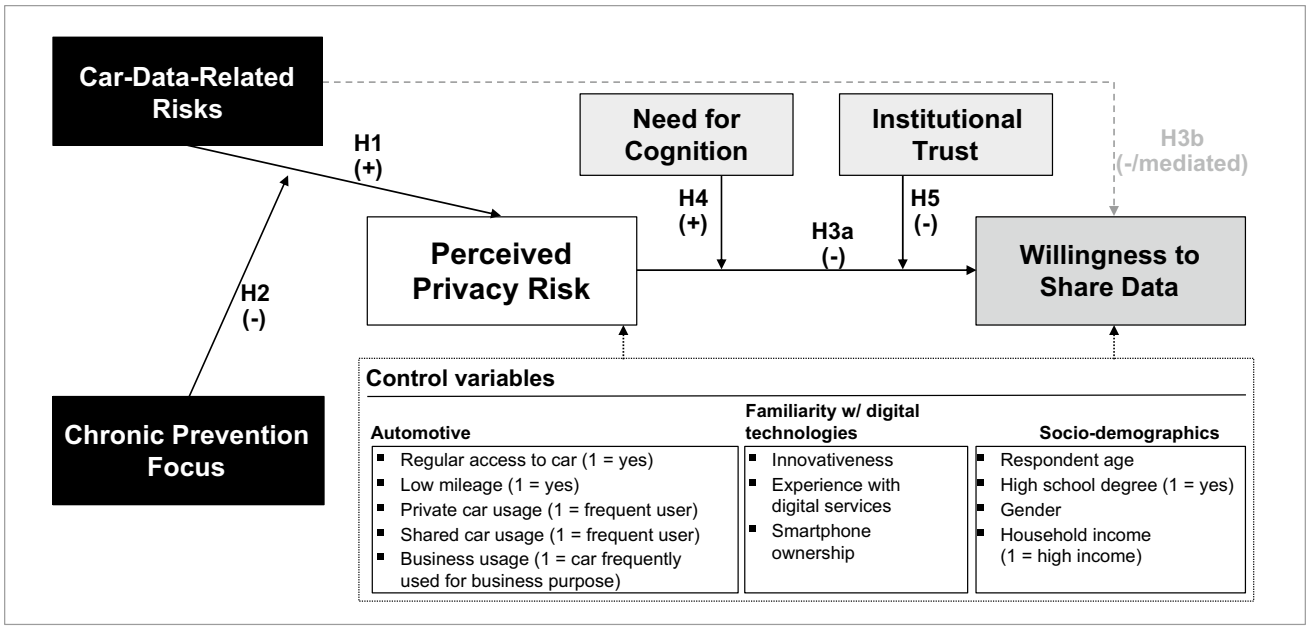

Fig. 1 Contextualized research model

reluctance of drivers to share data with the car manufacturer and other service providers (Cichy et al. 2021). We expect that the more likely drivers evaluate such negative consequences, the higher are their perceived privacy risks (Malhotra et al. 2004). Thus:

H1. *The more probable a driver considers car-data-related risks, the higher will be her perceived privacy risk.*

As explained before, risk beliefs form on the basis of two interacting components, namely individuals' evaluation of 1) the severity and 2) the likelihood of negative consequences. Certain consequences, though likely to occur, need not to be particularly severe and vice versa. We see strong arguments, that the perceived severity of negative consequences significantly differs between drivers. Based on their car data, one driver would be accused of misbehaving in road traffic while another driver would be attested to be a particularly considerate road user and always in compliance with traffic rules. Similarly, car data could reveal whether one's driving style is detrimental for vehicle health or – in case of a rental car – in accordance with the rental agency's conditions. Because there are many laws and rules for using cars and participating in road traffic, misbehavior is much more clearly defined than in other settings.

The extent to which drivers comply with relevant rules is structurally different across individuals and depend on their motivation to do so. Regulatory focus theory provides an explanation on interpersonal differences in this respect (Higgins 1998). The theory postulates that there are two regulatory systems that motivate human behavior, namely promotion-focus and prevention-focus. Individuals that tend to be promotion-focused are eager to maximize gains and are more willing to accept risky situations to avoid nongains, i.e., missing out on advantages. At the other end, prevention-focused individuals are motivated to avoid losses and are concerned with satisfying their security needs. They are said to be highly vigilant and try to behave safely to minimize negative outcomes (Chitturi et al. 2008).

Applied to the setting of driving a car, research revealed that prevention-focused individuals are less likely to engage in rule-breaking driving behavior such as speeding and passing other vehicles in dangerous circumstances (Hamstra et al. 2011). Driving safely and sticking to the rules assumingly helps them to fulfill their desire to avoid losses. We hence argue that drivers with a chronic – i.e., a habitual – prevention focus will have less to fear if their car data is disclosed as there is nothing much to criticize or sanction about how they treat the vehicle and behave in road traffic. They assumingly will evaluate negative consequences of car data disclosures, independent of how likely they assess these consequences in general, as less severe for them personally. We thus propose:

H2. *Chronic prevention focus will moderate the relationship of car-data-related risks on privacy risk, such that the negative effect will be weaker, the higher a driver's level of chronic prevention focus.*

Consequences of perceived privacy risk

Perceived privacy risk reduces an individual's intention to share personal information (Kehr et al. 2015; Krasnova et al. 2010). Hence, in the context of connected car services, we expect individuals to be less willing to share car data in exchange for a connected car service, if their perceived privacy risk is high. Thus, we hypothesize:

H3a. *The higher a driver's perceived privacy risk, the less willing she will be to share car data.*

Extant literature shows that privacy risk – despite of being conceptualized as a rather general perception of abstract risks associated with data sharing (e.g., Dinev et al. 2013) or as specific and contextualized risk assessment (Karwatzki et al. 2017) – have a negative effect on individuals' willingness to share personal data. However, no empirical study has interlinked both concepts as one being the determinant of the other. This is particularly surprising, as theory on the formation of risk beliefs, which we presented above, suggests that both conceptualizations are complementary rather than suited to be treated interchangeably. We argue that the anticipation of specific negative consequences will result in a broader concern about a loss of privacy associated with sharing car data that eventually will affect the data sharing decision. Hence, we devise the following mediation hypothesis:

H3b. *The more probable a driver considers car-data-related risks, the less willing she will be to share car data, with this link being mediated by her perceived privacy risk.*

Contingencies of perceived privacy risk

We further expect that the effect perceived privacy risk has on disclosure decisions is influenced by an individual's thinking style. Thinking style relates to preferences for either experiential or rational thinking and affects the deliberation as well as depth of individual's information processing (Shiloh et al. 2002). Need for cognition is a popular operationalization of thinking style and refers to the tendency to engage in and enjoy effortful cognitive activity (Epstein et al. 1996). Individuals with high need for cognition put more effort in searching, scrutinizing, and reflecting back on information in making sense of the world (Cacioppo and Petty 1982). In contrast, individuals low in need for cognition tend to rather rely on the opinions of credible others, judgmental heuristics, and social comparisons. Against this background it appears plausible, that high levels of need for cognition are associated with being confident about one's own thoughts and ideas (Wu et al. 2014) as well as with sticking more strongly to the beliefs and attitudes formed (Cacioppo et al. 1996). Individuals with this type of thinking style attach more weight to their own assessments, because these usually base on a rational and effortful assessment of information. This seems to be particularly true in the context of individual decision-making. Studies show, for example, that attitudes of individuals high in need for cognition were more predictive in the context of voting behavior than were the attitudes of those low in need for cognition (Cacioppo et al. 1986). Similarly, a study conducted by Lin et al. (2006) found that need for cognition moderates the effect of emotions and attitudes on individuals' risk-taking behavior.

In the context of privacy-related decisions, Dinev et al. (2015) argued that need for cognition invokes high-effort processing. High-effort processing in turn would alter how privacy risk perceptions influence actual data disclosure decisions. While scholars have argued that need for cognition affects the formation of perceived privacy risk directly (Kehr et al. 2015), we also see arguments for a moderating effect. Accordingly, we expect drivers with high need for cognition to rely even more strongly on the privacy-related risk beliefs they hold in deciding whether they want to reveal their car data in exchange for a service. Hence, we propose:

H4. *A driver's need for cognition will moderate the relationship of privacy risk on willingness to share car data, such that the negative effect will be stronger, the higher a driver's level of need for cognition.*

Several studies have found evidence for trust as a factor mitigating the effect of perceived privacy risk in privacy decisions (e.g., Kim 2008). In privacy research, trust is considered a belief positively influencing an individual's willingness to share personal data, as it embodies the expectation that another actor will not behave opportunistically (Dinev and Hart 2006). The exact positioning of trust and its role in privacy decisions have been inconsistent across extant privacy studies (Smith et al. 2011). Some scholars see trust as impacting willingness to disclose data independently of perceived privacy risk (Anderson and Agarwal 2011; Dinev and Hart 2004). Other studies model trust as an antecedent or as an outcome of beliefs about risk (Bansal and Gefen 2010). We, however, join the argumentation that trust affects an individual's willingness to accept risks (Venkatesh et al. 2016) rather than perceived privacy risk per se. Interpreting trust as an individual's accepted vulnerability to the trustee's intentions (Epstein et al. 1996), trust plays a key role in whether individuals overcome perceived privacy risk when confronting unfamiliar technologies (Harwood and Garry 2017). Thus, trust building has been identified as an important managerial strategy to increase users' willingness to use privacy-invasive services (Cichy et al. 2021), which is potentially more effective than reducing perceived privacy risk per se (Milne and Boza 1999) and more practical for service

providers to address. While some research (e.g., Krasnova et al. 2010) has analyzed how relational trust, i.e., trust towards the specific data-requesting stakeholder, impacts perceived privacy risk, we follow the argumentation of several studies (Dinev and Hart 2006; Kehr et al. 2015) that have measured institutional trust as a general tendency towards confidence in a data-collecting institution or actor (Kehr et al. 2015). We suggest that when individuals try to reduce cognitive complexity of the data sharing decision, they rely on their general trust beliefs towards a stakeholder group (such as car manufacturers or providers of connected services) rather than assessing the relational trustworthiness of the specific provider and their partners. This should especially be the case in the novel context of connected cars: Several connected car services such as intelligent parking services rely on different manufacturers and service providers working together to arrive at a critical mass of users and in order to realize all elements of the service delivery. The multitude of actors involved is assumingly difficult to oversee for individual users. Hence we conclude, that for individuals who generally trust that their data will not be misused by car manufacturers, perceived privacy risk will affect the willingness to share the requested data less strongly. We formulate:

H5. *A driver's institutional trust towards car manufacturers will moderate the relationship of privacy risk on willingness to share car data, such that the negative effect will be weaker, the higher a driver's level of institutional trust.*

Methods

Our empirical work consisted of two phases. First, we conducted a qualitative pre-study to refine the contextualized research model and to develop car-data-related risks as a novel and robust measure. The qualitative study involved context-immersive interviews with 33 participants following a hands-on driving experience in a connected car. This pre-study helped us to gain a deeper understanding of the concrete negative consequences individuals associate with connected cars and to identify further contextual factors of relevance for our research model. Second, our main study relied on data from a large-scale survey among 791 German car drivers to validate the contextualized research model.

Pre-study: Refining the contextualized research model and developing the multidimensional, contextualized privacy risk measure

Design and interview procedure We recruited 33 car drivers (age: min = 19 years, max = 83 years, M = 36.3 years, SD = 17.7; gender: M = 52% male; car usage: 49% frequent drivers) in Germany. We conducted context-immersive interviews that involved placing participants in the driver's seat of a connected car and interviewing them after showcasing the vehicle's advanced connectivity capabilities and associated services. The interviews were semi-structured with a focus on open questions (Flick, 2019). Before the actual interview, each participant received a 20-minute introduction to the technical background of connected cars and learned about the types of data the vehicle collects and processes. Using a 2018 SUV, several of its connected car features were demonstrated in action. Letting participants experience connected car services first-hand enhanced the validity of the subsequent semi-structured interviews.

Data analysis All interviews were digitally recorded (total length: 7.3 hours; M = 13.4 minutes, SD = 3.4) and completely transcribed (total interview material: 50,324 words; M = 1,525 words, SD = 366). We then conducted a content analysis of the verbatim interview transcripts (Miles and Huberman 1994) to derive categories and subcategories of negative consequences individuals associated with sharing car data. In a first step of open coding, we captured all text segments referring to negative consequences that respondents associate with connected cars and tagged them with exemplary quotes as so-called "in-vivo codes" (Strauss & Corbin, 1990). In a second step of data aggregation, we combined similar codes to inductively derive subcategories based on recurring types of negative consequences (Miles & Huberman, 1994). We discussed these subcategories with the author team and clustered them into broader main categories. In a third step, we performed axial coding (Strauss & Corbin, 1990) assigning the text segments to the subcategories across the interviews again. In a final step, we compared our categories and subcategories to extant privacy research. Our categories corresponded well to the seven privacy risk dimensions developed by Karwatzki et al. (2017). Furthermore, our subcategories closely matched the negative consequences associated with connected cars identified in extant research (Cichy et al. 2021). We decided to adopt the categorizations of Karwatzki et al. (2017) and (Cichy et al. 2021) to arrive at an integrated framework of privacy risk dimensions and specific negative consequences relevant in the connected car context.

Findings and Discussion The qualitative pre-study enabled us to generate deep insights on the negative consequences that drivers expect from sharing car data for using connected car services. At a broad level, our interviews highlighted the relevance of connected cars and IoT more generally as a meaningful setting for privacy research. At a more specific level, we unearthed 15 distinct negative consequences participants associated with the collection,

storage, and analysis of connected car data. These could be clustered into seven aggregate dimensions as shown in Table 1. The negative consequences cited included psychological consequences such as the fear of being overwhelmed while driving a connected car given the multitude of features and financial consequences arising from increased costs for car insurance due to tracking of driving behavior. For instance, as one respondent puts it: *"You will have to pay more for insurance, if you, for instance, drive 200 km/h on the motorway, even if it's legal." (Quote 22.1).* Respondents also discussed physical consequences, as criminals might use driving data to identify vulnerabilities, and may come to conclusions like *"Okay, this car is empty, or Mrs. XY is driving alone through the forest" (Quote 7.3)*, as one respondent speculated. They even anticipated risks for their career or social status, as data on poor driving might be used to stigmatize them or discriminate against them at work. One respondent stated: *"If somebody could see my driving data, like […] an employer, where I probably wouldn't be able to defend myself, I would find that bad" (Quote 15.5).* Interestingly, the far most frequently indicated risk was the fear of constant surveillance by unknown actors. As one respondent puts it: *"You're becoming more transparent and, well, you don't have an overview anymore of who can see you and where you are" (Quote 29.2).* This appears to be a point in favor of the abstract conceptualization of perceived privacy risk as a feeling of unease due to the loss of control over personal information. However, when asked for more detail, individuals explicated the more concrete negative consequences they associate with connected cars, as illustrated above. This observation is in line with our theoretical considerations regarding the interplay of concrete consequences and more abstract risk perceptions. In other words, we observed preliminary support for our first hypothesis, in which we expected individuals to base their privacy risk perceptions on the specific negative consequences they anticipated. While we chose a more real-life setting than (Cichy et al. 2021) and did not direct our respondents towards any negative consequences, we were able to reproduce the authors' findings on the various negative consequences associated with connected cars. As we sought to develop a multidimensional, contextualized privacy risk measure, we used the 15 risks identified and confirmed through our interviews to create items for our subsequent survey. More precisely, we formulated 15 potential scenarios that could happen to drivers of connected cars (see appendix 16 for the final measure). To develop a robust scale, we followed guidelines proposed by MacKenzie et al. (2011). In Appendix 17, we describe the scale development process in greater detail.

Moreover, our interviews pointed to a set of important context-specific variables to further contextualize our conceptual model (Hong et al. 2014). More specifically, our interviews unearthed several factors that might explain individual differences in drivers' perceived privacy risk and their willingness to share car data. These included a driver's age, smartphone ownership, and mobility habits. Based on these insights, we derived several context-specific covariates that we included as control variables in main study described below. Taken together, the qualitative findings helped to sharpen our understanding of how privacy risk perceptions are formed in the context of connected cars. We found broad support for our contention that individuals feel unease about the loss of control over their personal information given the concrete negative consequences that they associate with sharing car data. We were able to derive a novel, highly contextualized privacy risk instrument and to identify further contextual factors of relevance to be included in our contextualized research model.

Main study: Testing the refined contextualized research model

Design For our scenario-based online survey, respondents from Germany were recruited through invitations via email, social media posts, and messenger services. As an incentive for participation, we offered tickets for a raffle of vouchers for an online retailer.

Survey procedure The questionnaire consisted of three main parts. We introduced the respondents to the topic of connected cars. We asked respondents to imagine that their car was connected and that services were offered through its manufacturer. Then, participants were introduced to one of three randomly assigned connected car services: an app for searching for and booking parking spots (*SmartParking*), a driving style analysis app for real-time recommendations on eco-friendly driving behavior (*EcoDriver*), and a telematics-powered insurance product with discounts for considerate drivers (*Pay-how-you-drive Insurance*). We relied on short descriptions and illustrations of the services as stimuli, visualizing their value propositions, their technical features, and the types of driving data required for usage. Figure 2 shows an example of the stimuli used. We then measured our constructs starting with the dependent variable followed by the independent and control variables. For our final sample, we excluded 149 participants who showed unreasonable completion times or failed an attention check as well as 38 respondents under 18 years. This resulted in an overall sample size of 791 individuals, (mean age = 28 years, min = 18; max = 69; SD = 12.51; female = 55%, high school degree = 86%). While our sample was characterized by considerable diversity in terms of driver age and gender, it is not representative of the broader population of all German car

Table 1 Car-data-related risks reflected in our Interviews (n = 33)

PR Dimension[1]	**Car-data-related risk**[2]	**Privacy-invasive pratice**[3]	**Illustrative quote** (Respondent, quotation)
Psychological	Feelings of surveillance (in 14 of 33 interviews)	Collection	*"Of course, you always need to bear in mind that you're getting surveilled" (28.3); "You're becoming more transparent and, well, you don't have an overview anymore of who can see you and where you are" (29.2)*
	Distraction, feeling overwhelmed (8 of 33)	Collection	*"But this is distracting, as I realized. You are permanently thinking: 'Oh, OK, what do I need to do differently?'" (13.2); "How should I still focus on the street when there are so many features here, so many features there?" (23.1)*
Physical	Criminals identify vulnerabilities (8 of 33)	Collection	*"Okay, this car is empty, or Mrs. XY is driving alone through the forest" (7.3); "People are afraid that their data is analyzed, and anyone can know 'they're currently not at home" (14.4)*
	Manipulation of vehicle functions through hackers (6 of 33)	Unauthorized access	*"What if the car starts honking on the motorway, because someone hacked my car. […] Suddenly, the […] doors open while you drive" (30.2); "Or they take over steering…like in […] action movies" (23.3)*
Social	Stigmatization as potentially poor driver (2 of 33)	Collection	*"Well, well, well, Mrs. XY, you've been driving like a wild sow the entire way" (27.5); "Other family members may be able to track my driving style […] My wife already complains about my driving style when we are in the car together, I don't need more of that" (31.5)*
	Incorrect inferences from driving data (2 of 33)	Errors	*"You'll be blamed upfront. Although you might be totally uninvolved in the accident" (27.4); "If they want to find something you did wrong, they will find it, no matter if any driver would have handled the car in the same way" (28.7)*
Financial	Increased costs for car insurance (8 of 33)	Secondary use	*"You will have to pay more for insurance, if you, for instance, drive 200 km/h on the motorway, even if it's legal." (22.1); "I already heard about such insurance tariffs that are based on tracked driving behavior. It's optional at the moment, but I'm sure it will be mandatory soon, so they can earn more money" (15.3)*
	Enforced repair jobs (4 of 33)	Secondary use	*"They tell you: "You have to change brake pads, you have to do this and that" […] and the workshop does more than required" (14.5)*
	Loss of warranty (2 of 33)	Secondary use	*"Maybe I will be told that my driving style caused more wear and tear and thus they reject goodwill claims" (16.3); "Perhaps this is interpreted negatively for me, if they see I revved my engine too high while it was still in cold condition" (15.5)*

Table 1 (continued)

PR Dimension[1]	**Car-data-related risk**[2]	**Privacy-invasive pratice**[3]	**Illustrative quote** (Respondent, quotation)
Freedom-related	Unsolicited ads (5 of 33)	Secondary use	*"You will be bombarded with ads, as they know which shops you visit, etc." (7.4); "Take this car for instance: It's new, […], it's a Diesel, mileage is XY. You can figure 'okay, this is a field sales rep' and target your ads accordingly" (8.4)*
	Use of data for unintended purposes (5 of 33)	Secondary use	*"I wouldn't want that my data is sold to external providers, so they can adjust their sales activities" (8.5); "All rides are registered, and they'll know […] which restaurant I'm going to… I assume they sell this for advertising purposes" (18.4)*
	Data leaks (3 of 33)	Unauthorized access	*"The more companies possess my data, the more vulnerable is my data to […] hacker attacks" (5.6); "You don't necessarily want these data about you on the internet" (1.10)*
Prosecution-related	Automatized prosecution of traffic offenses (3 of 33)	Secondary use	*"I'd be concerned that someday all manufacturers are connected to the police […] and you automatically receive tickets" (33.3); "If you're constantly 10 km/h above the speed limit […], this could be reported to the police and you could get in trouble" (1.12)*
	Optimization of radar control position (2 of 33)	Secondary use	*"The police will know where people are speeding and will position their speed traps there to make the cash registers ring" (1.14); "The authorities might force manufacturer to give them car data so they know where people are going to fast" (22.4)*
Career-related	Disadvantages when performing driving jobs (2 of 33)	Secondary use	*"If somebody could see my driving data, like […] an employer, where I probably wouldn't be able to defend myself, I would find that bad" (15.5); "This could be really bad for, let' say, parcel carriers, that could be spied on by the employers, whether to comply to traffic rule or take too long breaks" (18.3)*

[1] Adapted from Karwatzki et al. 2018 [2] Adapted from Cichy et al. 2021 [3] Smith et al. 2011

drivers, which tends have a higher mean age, a lower share of female drivers, and a lower mean education level.

Measurement Figure 1 shows all dependent, independent, and control variables included in our main study. Car-data-related risks were measured using the scale we developed as part of the qualitative pre-study. To measure willingness to share car data, respondents answered the question, "Suppose the service is offered for your car: How willing are you to use the service and transmit the required driving data to the car manufacturer?" on a seven-point scale ranging from "not at all" to "extremely". All other main variables were captured through established measures from extant studies, as shown in the appendix. As our research relied on self-reported data, it is exposed to a potential common method bias (Podsakoff et al. 2003). We performed a confirmatory factor analysis and controlled for an unmeasured latent methods factor. Examining the structural parameters both with and without that factor in the model (Venkatesh et al. 2016), we found only marginal differences (i.e., a maximum delta of 0.02 between estimates) and gained confidence in the robustness of our findings.

Findings To test our hypotheses, we performed a multiple moderation analysis based on ordinary least squares path analysis (Hayes 2017) with heteroskedasticity-consistent standard errors (HC3, Davidson & MacKinnon, 1993; Hayes & Cai, 2007). For analysis, we used the software SPSS 25 and applied model 16 of the PROCESS extension. We established mediation by examining the indirect effects with boot-strapped data (10,000 samples). Table 2 shows our regression results, descriptive statistics can be found in

Fig. 2 Example for stimulus material used in survey

Appendix 16. We concluded that multicollinearity should not be an issue for our study variables, as no bivariate correlation between main constructs exceeded 0.5 (correlation between *Perceived Privacy Risk* and *Car-Data-related Risks*) respectively -0.68 for control variables (correlation between *Low Mileage* and *Regular Access to Car)*. Variance Inflation Factors (VIFs) were just slightly above 1 for all main constructs and not higher than just above 2 for control variables indicating little multicollinearity issues in our data.

Car-data-related risks were found to have a significant positive effect on perceived privacy risk ($B = 0.794$, $p < 0.01$), which is in support of H1. As the interaction term of car-data-related risks and chronic prevention focus is not significant ($B = 0.025$, $p = 0.583$), we could not support H2. Perceived privacy risk has a negative effect on willingness to share car data ($B = -0.654$, $p < 0.01$). Thus, H3a was supported. While we did not find a significant direct effect of car-data-related risks on willingness to share car data ($B = 0.070$, $p = 0.356$), we found a significant indirect effect on willingness to share car data via privacy concern ($B = -0.523$, 95% BC CI [-0.632, -0.425]). Thus, also Hypothesis 3b was supported. Need for cognition ($B = -0.163$, $p < 0.01$) and institutional trust ($B = 0.063$, $p < 0.05$) significantly moderate the relationship between perceived privacy risk and willingness to share car data (see Appendix C for plots of moderation effects). These findings are in support of H4 and H5.[1]

Regarding the context-specific control variables, some findings are worth noting. We found a significant negative effect of driver innovativeness on perceived privacy risk ($B = -0.114$, $p < 0.01$) as well as a significant positive effect of driver innovativeness on willingness to share car data ($B = 0.306$, $p < 0.01$). Put differently, as connected car services are a highly novel offering, drivers with high curiosity to test new products seem to be more willing to share car data and perceive a lower risk to their privacy by doing so. While we expected some user groups, i.e., drivers frequently using the car for business purposes or frequent users of car sharing, to be more willing to share car data, we did not find sufficient empirical support for such relationships. However, we found (female) gender to have a significant positive effect

[1] We were able to reproduce all findings by re-analyzing our data using PLS-SEM, where the weights of the 15 items of our formative car-related data index were estimated rather than treated as equal.

Table 2 Results from regression analysis

Independent variables		Dependent variables B (SE HC3)					
		Perceived Privacy Risk			Willingness to Share Data		
Main effects							
Car-Data-Related Risks		0.794	***	(0.048)	0.070		(0.075)
Chronic Prevention Focus		-0.142	***	(0.049)	0.057		(0.063)
Perceived Privacy Risk					-0.654	***	(0.051)
Institutional Trust					-0.050		(0.059)
Need for Cognition					-0.156	**	(0.051)
Interactions							
Chronic Prevention Focus X Car-Data-Related Risks		0.025		(0.045)			
Privacy Risk Perc. X Trust					0.063	**	(0.029)
Privacy Risk Perc. X Need for Cognition					-0.163	***	(0.032)
Control variables							
Automotive	Regular Access to Car	-0.129		(0.156)	0.335	*	(0.187)
	Low Mileage	-0.021		(0.146)	0.053		(0.174)
	Private Car Usage	-0.267	**	(0.131)	0.023		(0.177)
	Car Sharing Usage	0.177		(1.064)	-0.037		(0.907)
	Business Usage	0.233	*	(0.125)	-0.267		(0.173)
Familiarity with digital technologies	Innovativeness	-0.114	***	(0.046)	0.306	***	(0.060)
	Digital Experience	-0.031		(0.055)	-0.150	*	(0.086)
	Smartphone Ownership	0.775	*	(0.467)	0.193		(0.896)
Socio-Demographics	Age	0.006		(0.005)	-0.001		(0.006)
	High School Degree	0.181		(0.158)	0.126		(0.190)
	Gender	-0.097		(0.099)	0.312	**	(0.131)
	High Income	0.045		(0.147)	-0.125		(0.146)
Constant		4.209	***	(0.645)	2.258	**	(1.082)
R-squared		0.296			0.324		

Total observations = 791. Unstandardized estimates from Ordinary Least Squares (OLS) models. Heteroskedasticity-consistent standard error (HC3, Davidson and MacKinnon 1993; Hayes and Cai 2007) in parentheses. Chronic Prevention Focus, Perceived Privacy Risk, Institutional Trust, and Need for Cognition were mean centered before creating the interaction terms. * $p < 0.10$; ** $p < 0.05$; *** $p < 0.01$

on willingness to share car data ($B = 0.312$, $p < 0.05$). As female respondents were not found to perceive lower privacy risk, they might put less weight to these risk perceptions in their privacy decisions and are generally more willing to share car data.

Discussion and implications

Implications for research

Contextual contributions Our findings underscore that users anticipate far-reaching consequences of privacy invasion through connected cars as a particularly interesting IoT case. Importantly, we extracted a unique inventory of specific car-data-related risks that emerged from our context-immersive interviews. This inventory served as the basis for the development of a novel 15-item measurement instrument for users' car-data-related risks, which captures the specific nature of the negative consequences users associate with a loss of control over their car data. As we demonstrate based on our survey data, this measure is conceptually and empirically distinct from, yet predictive of, the more general construct of perceived privacy risk, which has been criticized for being too ambiguous (Li 2012) and too abstract (Karwatzki et al. 2018). Our results suggest that context-independent and context-specific privacy measures can complement instead of substitute each other when it comes to explaining the formation of privacy risk perceptions and data sharing decisions. We also find prevention-focused drivers to perceive lower privacy risk, as they, for instance, may adhere more strictly to traffic rules and are thus less severely exposed to negative consequences, when they share their car data. This means that IoT users form privacy risk

perceptions partially based on contextual rules and conditions that lie well beyond the actual technology and that were formulated without any reference to connected devices.

Conceptual contributions Considering different dimensions of risk helps privacy researchers to retrace how individuals form privacy risk perceptions. Importantly, information privacy and physical privacy appear to converge in the IoT in the eyes of users. It is uniquely forward-looking among the various types of risk, and uniquely concerned with loss of control. At their core, our theory and evidence extend our conceptual understanding of the process whereby privacy risk perceptions are formed and shape subsequent data sharing decisions. Importantly, we add to an emerging stream of research that draws on cognitive approaches to unearth individual contingencies (e.g., Brakemeier et al. 2016; Kehr et al. 2015). We make the case for incorporating chronic prevention focus especially for studies investigating contexts that are characterized by high regulation and long-term consequences. By considering an individual's level of prevention focus, we account for the fact that the perceived severity of car-data-related risks might well differ among drivers, depending on their tendency to comply with rules and norms. The same effects may be found in other IoT contexts: For example, disciplined users of smart health trackers might perceive fewer privacy risks, when they adhere to recommendations for lifestyle and regularly visit health exams. It is to be noted, however, that prevention-focused individuals may underestimate the personal severity of negative consequences from sharing car data, as scholars have found individuals to judge themselves to be significantly less exposed to privacy risk as they belief the broader group of users is (Cho et al. 2010; Baek et al. 2014). Our findings also show that need for cognition increases and institutional trust decreases the consideration of perceived privacy risk in data sharing decisions. For studies investigating connected devices and services, we advocate using institutional trust in IoT providers as opposed to relational trust towards the particular, customer-facing provider. In the IoT, services are frequently realized through an ecosystem of multiple providers (Porter and Heppelmann 2014). This is the case, for example, whenever additional services are purchased in a connected device's app store, or when different elements of the service value chain are delivered by different partners of the provider. Thus, IoT users need to trust in multiple actors handling their data responsibly. Our findings also imply that different thinking styles (characterized by one's need for cognition) and trust in institutions may explain part of the frequently observed "privacy paradox", i.e., inconsistencies between perceived privacy risk and data sharing behavior, and should thus be considered in privacy research models.

Methodological contributions Our study demonstrates the value of adopting a context-sensitive approach in IS research (Hong et al. 2014). This not only allowed for an exploration of the concrete, IS-specific negative consequences users associate with the collection, storage, and analysis of their data, but also helped in identifying further constructs to explain data sharing decisions, such as chronic prevention focus. Our context-immersive interviews provided a novel way of enhancing the validity of privacy research. In our study, they provided support and additional richness to a set of negative consequences individuals associate with connected cars identified in extant literature (Cichy et al. 2021). Importantly, the contextualized measure of car-data-related risks we derived from our qualitative data connects well with established measures in that it contains very similar categories of perceived risks (e.g., psychological risks, financial risks etc.) (e.g., Karwatzki et al., 2018). However, the specific perceived manifestations of these risk categories vary greatly between settings. This is where a contextualization is needed to complement more abstract measures of privacy risks. Our robust measure is not only readily available for further studies investigating the highly relevant connected car context, but can also guide the development of further multidimensional, context-specific privacy risk measures in other IS contexts.

Implications for practice and policy

Our study sheds new light on privacy issues that have remained unresolved and controversial in practice including the formation of privacy risk perceptions and individual differences in the determinants and consequences of these privacy risk perceptions (Lowry et al. 2017; Rai 2017). At a broad level, the findings from our context-immersive interviews and our survey provide policymakers and practitioners with an overview of the negative consequences connected car users worry about along with the perceived likelihood of these negative consequences. This might help to prioritize which areas of concerns to address, such as through privacy policies and communicative measures. For instance, financial risk like losses of warranty and freedom-related risks like unsolicited ads, are shown to be top concerns of connected car users. Service providers may rigorously exclude data use for these purposes in their terms and conditions, and explicitly communicate to their customers that car data will never be used for review of warranty claims or transmitted to service partners for promotional use. Moreover, service providers may pay close attention to develop services, so they work with a minimum of data and collect no more than needed. However, there will be a trade-off between data-minimal service design and leaving enough room for data usage opportunities that might not be apparent yet. Notably, not all the risk perceptions that individuals may have

are fully reasonable, as legal safeguards and cybersecurity measures that are currently in place may effectively reduce the probability of certain privacy threats to a minimum. For practitioners, it may be especially insightful to review the delta between the perceived privacy risk of users and the actual privacy risks to learn which risks are overestimated and which are underestimated by users.

Our study also shows that policies can play a central role in customers' acceptance of connected car services – not only those directly affecting connected car services by regulating their privacy-invasive practices, but also those that create the broader regulations around using cars in general. As a case in point, our findings on chronic prevention focus imply that considerate car drivers might tend to be more willing to use connected car services, as they will be less exposed to negative consequences arising from traceable rule violations. Such selection effects might be considered good news for providers of services like pay-how-you-drive telematic insurance schemes. For other services, however, service providers could signal that recorded driving behavior will not be used against their customers' interests, as this appears to be a key concern.

Our findings further help to identify design strategies for service providers seeking to increase consumers' willingness to share data. Providers could adapt their devices and services to cater to the thinking style of users. Flexible privacy settings and understandable information on how the information is used (Kehr et al. 2015) – not hidden in the terms ans conditions section, but well-visible and transparently explained – may appeal to users with a high need for cognition, who, as we found, ascribe more importance to the perceived privacy risk in their data sharing decisions. As our study found that trust in institutions – here, car manufacturers in general – attenuates the effect of perceived privacy risk, we advise service providers to foster industry standards for responsible collection, processing, and usage of personal data, and demonstrate these standards to their customers, such as in the form of externally-validated privacy seals (Kim 2008). This appears particularly important in the context of connected devices, where services are often delivered through an ecosystem of providers.

Limitations and future research

Our study is subject to several limitations that offer fruitful avenues for future research. First, our survey employs a hypothetical scenario, instead of measuring actual usage behavior. As explained above and commonly referred to as "privacy paradox" (Alashoor et al. 2018), disparities between perceived privacy risk and actual data sharing behavior may persist. We partly addressed this in our pre-study by using a realistic connected car setting with a live demonstration. Still, future research would benefit from experimental setups observing actual disclosure behavior. A further constraint of our study lies in the geographic context of Germany, as the research may be impacted by cultural and societal specifics. We also point out that our survey sample is not representative of the population in terms of age and education level. The same holds true for the interviews of our pre-study: While we are confident to have reached adequate saturation in our exploration of negative consequences and to have established adequate validity in our novel construct car-data-related risks, we explicitly encourage replication studies, especially of a comparative cross-country nature. Such studies would ideally adopt longitudinal or controlled experimental designs to have a sufficient empirical basis for disentangling true causation from mere correlation. Scholars seeking to further enhance contextualized, multidimensional privacy risk measures could complement our approach by considering both the perceived likelihood and severity of negative data-related consequences. Likewise, future research might want to go beyond our focus on perceived risks, by including measures of perceived data-related benefits, potentially manipulating these benefits across experimental groups, and examining the interplay between users' data-related risk and benefit perceptions.

Conclusion

The connected car is a particularly insightful example of how the IoT provides users with an enhanced product experience, but also with novel privacy risks. Responding to calls for a more context-specific, multidimensional investigation of privacy risk, we unearth the specific nature of connected car drivers' perceptions of privacy risk as they relate, for instance physical safety, their financial resources, their social status, and their freedom. We show that such a contextualized measure of car-data-related risks predicts users' perceived privacy risks at a more abstract level, which in turn shape their willingness to share car data. Importantly, we found that the effect of drivers' privacy risks on their willingness to share their car data varies between drivers. As data sharing decisions are cognitively demanding processes and connected cars are a particularly complex context, we find that drivers with a high need for cognition give more weight to perceived privacy risk, while trust in car manufacturers reduces the effect of perceived privacy risk. Overall, more granular insights into the formation, consequences, and contingencies of perceived privacy risk appears valuable for privacy researchers to understand users' data sharing decisions, for practitioners to develop adequate services, and for policy makers to put the right safeguards in place.

Appendix A

3, 4

Table 3 Contextualized construct measures

Perceived Privacy Risk* (adapted from Dinev et al. 2013; CA = 0.87; CR = 0.87, AVE = 0.63)
The collection and processing of personal driving data through the connected car service…

1. is risky in general.
2. is associated with a high potential for loss of my privacy.
3. could involve many unexpected problems.
4. could involve inadequate usage of my data.

Chronic Prevention Focus* (adapted from Haws et al. 2010; CA = 0.68; CR = 0.80; AVE = 0.53)

1. I frequently think about how I can prevent failures in my life.
2. I worry about making mistakes.
3. I see myself as someone who is primarily striving to become the self I "ought" to be — to fulfill my duties, responsibilities and obligations.
4. I usually obeyed rules and regulations that were established by my parents.

Institutional Trust* (adapted from Malhotra et al. 2004; CA = 0.88; CR = 0.88; AVE= 0.72)

1. Car manufacturers would be trustworthy in handling customer data.
2. Car manufacturers are honest with customers when it comes to using the information that I would provide.
3. Car manufacturers would tell the trust and fulfill promises related to the information provided by me.

Need for Cognition* (adapted from Epstein et al. 1996; CA = 0.77; CR = 0.84; AVE = 0.57)

1. Thinking hard and a for a long time about something gives me little satisfaction. (R: reverse coded)
2. I prefer to do something that requires little thought rather than something that challenges my thinking abilities. (R)
3. I prefer to think about small, everyday undertakings rather than about long-term plans. (R)
4. I think just as hard as I need to. (R)

Car-data-related Risks** (self-developed) *How do you assess the likelihood of occurrence of the following scenarios?*

[Psychological risks]
1. Drivers increasingly feel surveilled and fully transparent.
2. Drivers feel overwhelmed by complexity of data and information flows of connected cars.

[Career-related risks]
3. Professional drivers face disadvantages when applying for or performing driving jobs (e.g., when excessive breaks or traffic offences can be proven).

[Prosecution-related risks]
4. Police uses driving data to impose prosecution, fines, or loss of driving license in the event of recorded misbehavior.
5. Data of connected cars is used to identify streets with frequent speeding and, in turn, to optimize positioning of radar speed checks.

[Financial risks]
6. Connected car owners lose warranty services for the vehicle (e.g., when improper handling is recorded).
7. Drivers see disadvantages when insuring or renting a car (e.g., for risky driving style) and face liability issues in case of self-inflicted car accident.
8. Car manufacturer performs digital manipulations to stimulate spending on car maintenance and repair.

[Physical risks]
4. Criminals use driving data to identify daily routines and vulnerabilities (e.g., burglars might find out when no one is at home or know that car is usually not locked when parked in one's private garage).
5. Hackers manipulate vehicle functions (e.g., window lifts, breaks).

[Social risks]
6. Drivers are stigmatized as bad drivers.
7. Data is assigned to the wrong driver and incorrect inferences from driving data are drawn (e.g., in case of a company car or when car is shared among family members).

[Freedom-related risks]
8. Car manufacturer (mis)use shared driving data for unexpected purposes or resale the data to other companies.
9. Increase of unsolicited advertisement and rebate offerings by car manufacturers.
10. Criminals steal or manipulate driving data (e.g., through data leaks, hacker attacks).

All items measured by seven-point scales. *Anchored by "strongly disagree" and "strongly agree"; **anchored by "unrealistic" and "realistic". CA = Cronbach's alpha; CR = composite reliability; AVE = average variance extracted; (R) = item was reverse coded. For our novel construct Car-data-related Risks which we specified as an index with formative indicators, common measures for validity and internal consistency are not appropriate (Diamantopoulus & Winklhofer 2001). Based on our qualitative study, we however found confidence in the adequate validity.

Table 4 Descriptive statistics and bBivariate correlations

				Bivariate correlations															
		M	SD	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	Willingness to share data	4.5	2.0	-																
2	Car-data Related Risks	4.9	1.0	-0.16**	-															
3	Chronic Prevention Focus	4.9	1.1	0.10**	0.16**	-														
4	Perceived Privacy Risk	4.5	1.5	-0.48**	0.50**	0.01	-													
5	Inst. Trust	3.4	1.3	0.19**	-0.30**	0.10**	-0.35**	-												
6	Need for Cognition	4.8	1.3	-0.12**	-0.05	-0.13**	0.05	-0.20**	-											
7	Regular Access to Car	0.8	0.4	0.01	0.02	-0.06	-0.01	0.00	0.06	-										
8	Low Mileage	0.4	0.5	0.02	-0.02	0.10**	-0.01	-0.01	-0.03	-0.68**	-									
9	Private Car	0.3	0.4	-0.02	0.05	-0.06	-0.01	-0.03	0.02	0.30**	-0.39**	-								
10	Car Sharing Usage	0.0	0.1	0.001	0.03	0.07*	0.02	0.10*	-0.08*	0.04	-0.02	0.12**	-							
11	Business Usage	0.3	0.5	-0.06	0.03	-0.09**	0.04	0.02	0.05	0.30**	-0.39**	0.47**	0.05	-						
12	Innovativeness	4.6	1.1	0.16**	0.01	0.04	0.01	-0.01	0.13**	-0.01	-0.02	0.02	0.01	0.02	0.18**	-				
13	DigitalExperience	3.0	0.8	-0.02	0.01	0.04	0.01	-0.01	0.13**	-0.01	-0.02	0.02	0.01	0.02	0.18**	-				
14	Smartphone Ownership	1.0	0.1	0.06	-0.03	-0.05	0.01	0.00	0.00	0.01	-0.02	0.01	-0.01	0.08*	0.07*	-				
15	Age	28.	12.5	-0.09**	0.09**	-0.19**	0.09**	-0.12**	0.05	0.22**	-0.27**	0.20**	0.13**	0.24**	-0.09**	-0.17**	-0.09**	-		
16	Highschool	3.8	0.5	0.02	-0.03	-0.03	-0.03	-0.06	0.14**	-0.07*	-0.14**	-0.01	-0.09**	0.04	0.14**	0.05	-0.25**	-		
17	Gender (Female)	0.6	0.5	0.07*	0.13**	0.07*	0.04	0.02	0.04	0.00	0.03	0.02	-0.02	-0.06	-0.05	-0.17**	0.02	0.000	-0.06	-
18	High Income	0.2	0.4	-0.02	-0.04	0.13**	-0.01	-0.04	0.12**	0.20**	-0.24**	0.12**	-0.03	0.20**	0.01	0.01	0.02	0.39**	-0.01	-0.08*

Appendix B

Developing the construct car-data-related risks – detailed development process

To develop a robust scale using the 15 negative consequences of connected cars identified as items, we followed guidelines proposed by MacKenzie et al. (2011). First, and in line with Karwatzki et al. (2017), we conceptualized the construct car-data-related risks as the extent to which an individual believes that specific negative consequences may arise from sharing car data. Based on the work of (Cichy et al. 2021), these consequences are the result of privacy-invasive practices of connected car services, i.e., the secondary use of, the collection of, and the unauthorized access to personal data, as well as errors in processing that data. In line with Karwatzki et al. (2018), we expect negative consequences to manifest in physical, social, resource-related, psychological, prosecution-related, freedom-related and career-related ways. We formulated 15 potential scenarios that could happen to drivers of connected cars based on our interview findings and the 15 risks identified by (Cichy et al. 2021). Deploying this measure in our survey, we asked respondents to assess the likelihood of each of these 15 scenarios on a seven-point scale anchored by "unrealistic" and "realistic" (see appendix 18). As noted above, we were able to reproduce the findings of (Cichy et al. 2021) on the various negative consequences associated with connected cars, although the design and setting of our context-immersive interviews differed significantly. Also, we were able to replicate the seven dimensions of privacy risk from Karwatzki and colleagues (2017) propose. For these reasons, we felt confident in the validity of our measure. Second, we evaluated the formal specification of our measurement model (MacKenzie et al. 2011). While all 15 risks identified can be linked to the seven privacy risk dimensions (Karwatzki et al., 2017), the indicators are conceptually different and do not necessarily covary (Jarvis et al. 2003). For instance, both feeling of surveillance and feeling of being overwhelmed are psychological risks, but they are conceptually different and not interchangeable, as they cover different aspects of psychological risk that do not necessarily covary. In other words, while users with an affinity for digital innovation may find it easy to navigate connected car services and perceive little risk of being overwhelmed by the features, they may still be concerned about surveillance through connected car services. Vice versa, users finding it difficult to adapt to new applications may not worry that their data could be used to spy on them. As the seven privacy risk dimensions are distinctive categories of negative consequences (Karwatzki et al., 2018), we specify the construct car-data-related risks as a simple index with formative indicators (Diamantopoulos and Winklhofer 2001). This specification sees the construct as an explanatory combination of indicators (Fornell and Bookstein 1982) and conceives the 15 risks identified as a collectively exhaustive set capturing the domain (Diamantopoulos and Winklhofer 2001) of negative consequences associated with connected cars. In our main analyses, all 15 risks were equally weighted. As we show, however, as part of our robustness checks, our findings are consistent to including individually estimated item weights in structural estimation modelling setup.

Appendix C

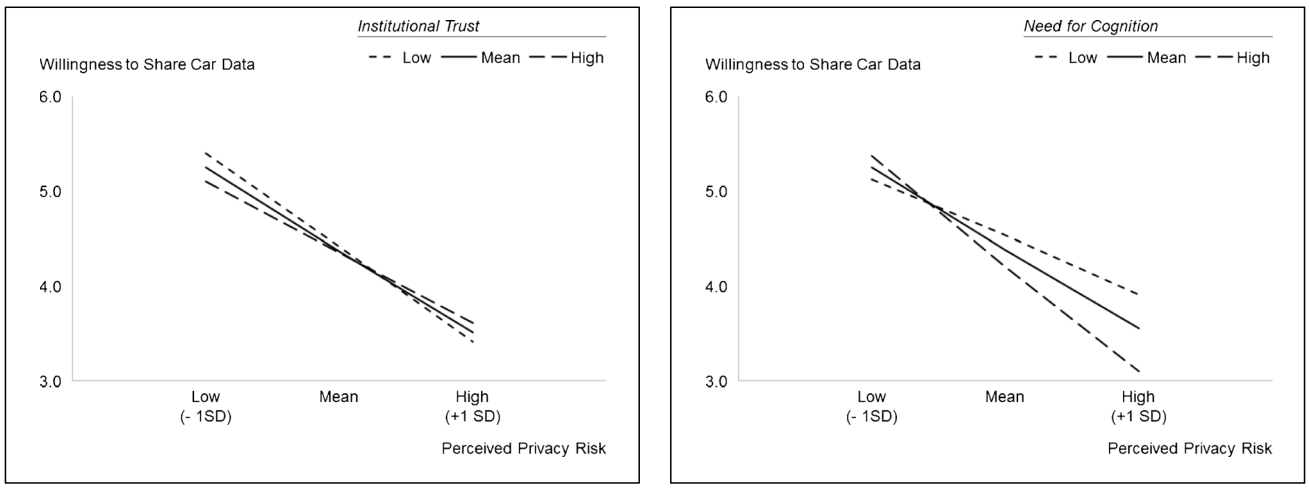

Fig. 3 Moderation of the effect of perceived privacy risk on willingness to share data at values of the moderators and Conditional indirect effect of Car-Data-Related Risks on Willingness to Share Data at values of the moderators

Appendix D

Table 5 and 6

Table 5 Literature considering privacy risks

Authors (Year)	Study context	Research objective	Conceptualization of privacy risk	Scale adapted from	Methodology
Brakemeier et al. (2016)	Online social networks	Investigate the role of regulatory focus in the privacy calculus	Perceived risks of information disclosure as cost side of privacy calculus	4 items reportedly adopted from Heng et al. (2011); equivalent to Malhotra et al. (2004); wording contextualized to Facebook app	Experiment
Cazier et al. (2008)	Stationary retail	Study the factors that influence customers' intention to use radio frequency identification technologies (RFID)	• Perceived Privacy Risk constructed of two components: Perceived privacy risk likelihood and perceived privacy risk harm • "Risk likelihood is the perception of the probability that a privacy breach will occur" • "Risk harm is the perception of the level of damage that would occur in the event of a privacy breach"	Self-developed scales, 3 synonymous items each for likelihood and harm	Survey
Chen (2013)	Online social networks	Identify key stimuli and inhibitors of member self-disclosure in social networks	Perceived internet risk: "measures one's uneasiness about using the Internet"; "reflects prior experience with regards to the immediate surrounding computing environments of social networking sites"	3 items reportedly adapted from Grazioli (Jarvenpaa) et al. 2000, equivalent to Malhotra et al. (2004): "generally would be risky", "unexpected problem", "feel unsafe"	Survey
Cocosila et al. (2009)	eHealth	Study acceptance factor for wireless text messaging on cell phones to improve user adherence to healthy behavior	• Risk in consumer behavior as starting point: Perceived privacy risk as an antecedent of psychological risk, next to social and financial risk • Perceived privacy risk as "uncertainty or fear that online businesses may use inappropriately customer personal information" (Featherman and Pavlou 2003)	Perceived privacy risks; 3 items adapted from Featherman and Pavlou (2003); not modified/contextualized	Experiment
Featherman & Pavlou (2003)	Electronic payment services	Investigate types of risk perceptions and their impact on e-services adoption decision	Perceived risk: "the potential for loss in the pursuit of a desired outcome of using an e-service"	• Prior studies from the authors (Featherman 2001 & Pavlou 2001) • 3 items: chances of 1) loss of control 2) loss of privacy 3) hacker attack	Quasi-experiment

Table 5 (continued)

Authors (Year)	Study context	Research objective	Conceptualization of privacy risk	Scale adapted from	Methodology
Grazioli and Jarvenpaa (2000)	Online shopping	Investigate how well experienced Internet shoppers can detect new forms of seller deception	Perceived risk: "consumer's perceptions of uncertainty and adverse consequences of engaging in an activity" (Downling & Staelin 2000)	• 3 items as found in Jarvenpaa et al. (1999) and Jarvenpaa and Tractinsky (1999): Opportunity vs. Risk, high potential for loss or gain, positive situation or negative situation and overall perception ("I feel this transaction is risky") • Contextualized/situation-specific	Laboratory experiment
Karwatzki et al. (2018)	eHealth	Develop a multidimensional privacy risk to capture the specific negative consequences feared by individuals when their privacy is invaded	• Privacy risk: "extent to which an individual believes that negative outcomes may arise from others' access to his or her personal information" • 7 dimensions of privacy risk: physical, social, resource-related, psychological, prosecution-related, career-related and freedom-related risks • Specific to given context and situation	• Utilization of items from existing risk scales: e.g., Featherman and Pavlou, 2003; Krasnova et al., 2010 • Contextualized ("this app"), but not to specific consequences	Survey
Krasnova et al. (2010)	Online social networks	Investigate users' motivation for disclosure of personal information on social networks	• Perceived privacy risk • Argumentation following Malhotra et al. (2004): Privacy risk entails privacy concerns as a dispositional antecedent, thus decided for privacy risk as construct used	• 5 items adapted from Malhotra et al. 2004 • Contextualized to OSN • Directly asking for privacy risk (in contrast to Malhotra) • 3 items eventually used: "threat to my privacy", "perception of privacy risk", "feel safe publishing information"	Survey
Wu et al. (2014)	Mobile advertising	Investigate the effect of pull/push information delivery in the efficacy of privacy intervention approaches in influencing privacy decision making	• Privacy risk = "expectation of losses associated with the release of personal information to the [service] provider" • Privacy risk as another facet of risk next to performance, financial, time, safety, social, psychological (not included here; Featherman & Pavlou 2003)	3 items adapted from Malhotra et al. (2004)	Quasi-experiment

Table 6 Literature considering privacy risks and privacy concerns

Authors (Year)	Study context	Research objective	Conceptualization of privacy concerns	Privacy concern scale adapted from	Conceptualization of privacy risk	Privacy risk scale adapted from	Methodology
Alashoor et al. (2018)	Online social networks	Examine if/how affect (i.e., positive and negative mood states) interrupt the privacy calculus	"Users' dispositional worry about the way their personal information is treated in terms of collection, improper and secondary use, control, and errors"	4 items adapted from Dinev and Hart (2006); all items used, wording adapted to social media websites	"Cognitive expectations of a loss associated with disclosing personal information"; situation-specific	5 items adapted from Malhotra et al. (2004); all items used, wording adapted to social media websites	Quasi-experiment
Dinev and Hart (2006)	eCommerce	Shed light on privacy paradox by better understanding the predictorsof a user withholding or surrendering personal-information when using the Internet	• Internet privacy concerns: "Concerns about opportunistic behavior related to the personal information submitted over the Internet by the respondent in particular" • Individual's assessment on personal level	• New scale, based on items from Smith et al. (1996) and Culnan & Armstrong (1999) • 4 items covering privacy practices related to collection, unauthorized secondary use, and improper access	• Perceived internet privacy risk: "Collective risk for internet users: Perceived risk of opportunistic behavior related to the disclosure of personal information submitted by Internet users in general" • Individual's assessment on collective level	• Scale from Dinev & Hart 2004 • 4 items covering resale to third parties, misuse, unauthorized sharing to unknowns, sharing with government agencies	Survey
Hong et al. (2013)	eCommerce; governmental websites	Integrate existing privacy concerns measures to create a comprehensive, six-dimensional Internet Privacy Concerns (IPC) scale	• Internet privacy concerns • Focus on individuals' perceptions of these concerns rather than expectations	• New scale using items from: Smith et al. (1996) and Malhotra et al. (2004) • 3 factors: Interaction management (collection, secondary use, control), information management (errors and improper access), awareness	Risk beliefs	Malhotra et al. (2004)	Survey
Kehr et al. (2015b)	Connected cars (smartphone application)	Explore the dynamics of pre-existing factors (general privacsy concerns, general institutional trust) and mood of situation-specific privacy calculus	General privacy concerns = "individual's general tendency to worry about information privacy" (Li et al. 2011)	4 items adapted from Dinev and Hart (2006); not context-specific	Perceived risks of information disclosure = "potential for loss associated with the release of private information" (Smith et al. 2011)	4 items adapted from Dinev et al. (2012); contextualized to provider of respective smartphone application	Experiment

Table 6 (continued)

Authors (Year)	Study context	Research objective	Conceptualization of privacy concerns	Privacy concern scale adapted from	Conceptualization of privacy risk	Privacy risk scale adapted from	Methodology
Koohika-mali et al. (2015)	Online social networks (location-based)	Investigate how marketers can motivate people to disclose their location despite their awareness of risks	• Close to IUIPC • Calling for context-specific conceptualization	• Self-developed 8-item scale based on items from Chen 2013, Buchanan et al. 2007 and Xu et al. 2008, mix of general privacy perception and location-based service specific concerns • Some items formulated specific to context (type of information, potential consequences)	• Perceived risk • "Users' beliefs about potential negative outcomes from the use of LB-SNAs" (adapted from Malhotra et al. 2004)	• Malhotra et al. (2004) (items quoted from Chen (2013), Grazioli et al. (2000)) • Contextualized to location-based services in general, not specific service in study	Survey
Malhotra et al. (2004)	eCommerce; Digital Marketing	Develop new scale to measure Internet Users' Information Privacy Concerns (IUIPC)	• IUIPC: "degree to which an Internet user is concerned about online marketers' collection of personal information, the user's control over the collected information, and the user's awareness of the collected information is used" • Focus on individuals' perceptions of fairness/justice	• New scale; second-order construct with three dimensions: control (3 items), awareness (3 items), and collection (4 items) Items developed based on Smith et al. (1996); contextualized to internet and online companies	• Risk beliefs = "expectation that a high potential for loss is associated with the release of personal information to the firm" (Dowling and Staelin 1994) • Privacy notion	• Adapted from Jarvenpaa and Tractinsky (1999); some items newly developed • Contextualized to online companies in general (institutional level)	Interviews, survey
Okazaki et al. (2009)	Mobile advertising	Assessment the consequences of individuals' privacy concerns in the context of mobile advertising	Mobile Users' Information Privacy Concerns; following IUIPC	Malhotra et al. (2004); contextualized to mobile advertisers	Perceived risk in mobile advertising: "extent to which users are uncertain about the negative consequences of opening, reading, or responding to mobile advertising"	Malhotra et al. (2004), not contexualized ("online companies" in general)	Quasi-experiment

Table 6 (continued)

Authors (Year)	Study context	Research objective	Conceptualization of privacy concerns	Privacy concern scale adapted from	Conceptualization of privacy risk	Privacy risk scale adapted from	Methodology
Van Slyke et al. (2006)	eCommerce	Assess the impact of consumers' concerns for information privacy on their willingness to engage in online transactions	CFIP, not contextualized	Smith et al. (1996), Stewart and Segars (2002)	• Risk perception: "Individual's belief regarding the probability of gains or losses associated with purchasing goods or services from a Web merchant" (Mayer et al., 1995) • Not limited to privacy • Specific to online merchant	Jarvenpaa et al. (2000; same scale in Grazioli and Jarvenpaa 2001)	Survey
Xu et al. (2008)	Website usage	Investigate how individuals form privacy concerns	Privacy concerns "as the proxy to define and measure the concept of privacy"	5 items adapted from Smith et al. (1996); 1 item taken per dimension	Perceived privacy risk "as the expectation of losses associated with the disclosure of personal information online"	Dinev & Hart (2006) and Malhotra et al. (2004)	Survey

Funding Open Access funding enabled and organized by Projekt DEAL.

References

Alashoor, T., Al-Maidani, N., & Al-Jabri, I. (2018). The privacy calculus under positive and negative mood states. *Proceedings of the International Conference on Information Systems (ICIS).*

Anderson, C. L., & 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. https://doi.org/10.1287/isre.1100.0335

Baek, Y. M., Kim, E. M., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior, 31*, 48–56. https://doi.org/10.1016/j.chb.2013.10.010

Bansal, G., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138–150. https://doi.org/10.1016/j.dss.2010.01.010

Bearden, W. O., & Mason, J. B. (1978). Consumer-perceived risk and attitudes toward generically prescribed drugs. *Journal of Applied Psychology, 63*(6), 741. https://doi.org/10.1037/0021-9010.63.6.741

Brakemeier, H., Widjaja, T., & Buxmann, P. (2016). Calculating with different goals in mind–the moderating role of the regulatory focus in the privacy calculus. *Proceedings of the 24th European Conference on Information Systems (ECIS).*

Cacioppo, J. T., Petty, R. E., Feinstein, J. A., & Jarvis, W. B. G. (1996). Dispositional differences in cognitive motivation: The life and times of individuals varying in need for cognition. *Psychological Bulletin, 119*(2), 197. https://doi.org/10.1037/0033-2909.119.2.197

Cacioppo, J. T., Petty, R. E., Kao, C. F., & Rodriguez, R. (1986). Central and peripheral routes to persuasion: An individual difference perspective. *Journal of Personality and Social Psychology, 51*(5), 1032. https://doi.org/10.1037/0022-3514.51.5.1032

Cacioppo, J. T., & Petty, R. E. (1982). The need for cognition. *Journal of Personality and Social Psychology, 42*(1), 116. https://doi.org/10.1037/0022-3514.42.1.116

Cichy, P. S., Torsten, O., Kohli, R. (2021). Privacy concerns and data Sharing in the internet of things: *Mixed Methods Evidence from Connected Cars MIS Quarterly, 45*(4) pp 1863–1892.

Chitturi, R., Raghunathan, R., & Mahajan, V. (2008). Delight by design: The role of hedonic versus utilitarian benefits. *Journal of Marketing, 72*(3), 48–63. https://doi.org/10.1509/JMKG.72.3.048

Cho, H., Lee, J.-S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior, 26*(5), 987–995. https://doi.org/10.1016/j.chb.2010.02.012

Cox, D. F., & Rich, S. U. (1964). Perceived risk and consumer decision-making—the case of telephone shopping. *Journal of Marketing Research, 1*(4), 32–39. https://doi.org/10.1177/002224376400100405

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Davidson, R., & MacKinnon, J. G. (1993). Estimation and inference in econometrics. *OUP. Catalogue.*

Diamantopoulos, A., & Winklhofer, H. M. (2001). Index construction with formative indicators: An alternative to scale development. *Journal of Marketing Research, 38*(2), 269–277. https://doi.org/10.1509/jmkr.38.2.269.18845

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology, 23*(6), 413–422. https://doi.org/10.1080/01449290410001715723

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box. *Information Systems Research, 26*(4), 639–655. https://doi.org/10.1287/isre.2015.0600

Dinev, T., Xu, H., Smith, J. H., & 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, G. R. (1986). Perceived risk: the concept and its measurement. *Psychology & Marketing, 3*(3), 193–210. https://doi.org/10.1002/mar.4220030307

Epstein, S., Pacini, R., Denes-Raj, V., & Heier, H. (1996). Individual differences in intuitive–experiential and analytical–rational thinking styles. *Journal of Personality and Social Psychology, 71*(2), 390.

Fornell, C., & Bookstein, F. L. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of Marketing Research, 19*(4), 440–452. https://doi.org/10.1177/002224378201900406

Glover, S., & Benbasat, I. (2010). A comprehensive model of perceived risk of e-commerce transactions. *International Journal of Electronic Commerce, 15*(2), 47–78. https://doi.org/10.2753/JEC1086-4415150202

Hamstra, M. R. W., Bolderdijk, J. W., & Veldstra, J. L. (2011). Everyday risk taking as a function of regulatory focus. *Journal of Research in Personality, 45*(1), 134–137. https://doi.org/10.1016/j.jrp.2010.11.017

Harwood, T., & Garry, T. (2017). Internet of Things: understanding trust in techno-service systems. *Journal of Service Management, 28*(3), 442–475. https://doi.org/10.1108/JOSM-11-2016-0299

Hayes, A. F., & Cai, L. (2007). Using heteroskedasticity-consistent standard error estimators in OLS regression: An introduction and software implementation. *Behavior Research Methods, 39*(4), 709–722.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105. https://doi.org/10.2307/25148625

Higgins, E. T. (1998). Promotion and prevention: Regulatory focus as a motivational principle. *Advances in Experimental Social Psychology, 30*, 1–46. https://doi.org/10.1016/S0065-2601(08)60381-0

Hong, W., Chan, F. K. Y., Thong, J. Y. L., Chasalow, L. C., & Dhillon, G. (2014). A framework and guidelines for context-specific theorizing in information systems research. *Information Systems Research, 25*(1), 111–136. https://doi.org/10.1287/isre.2013.0501

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research, 30*(2), 199–218. https://doi.org/10.1086/376806

Jozani, M., Ayaburi, E., Ko, M., & Choo, K.-K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior, 107*, 106260. https://doi.org/10.1016/j.chb.2020.106260

Karwatzki, S., Trenz, M., Tuunainen, V. K., & Veit, D. (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.

Karwatzki, S., Trenz, M., and Veit, D. (2018). Yes firms have my data but what does it matter - Measuring privacy risks. *Proceedings of the 26th European Conference on Information Systems (ECIS),* Portsmouth.

Keh, H. T., & Sun, J. (2008). The complexities of perceived risk in cross-cultural services marketing. *Journal of International Marketing, 16*(1), 120–146. https://doi.org/10.1509/jimk.16.1.120

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal, 25*(6), 607–635. https://doi.org/10.1111/isj.12062

Kim, D. J. (2008). Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study. *Journal of Management Information Systems, 24*(4), 13–45. https://doi.org/10.2753/MIS0742-1222240401

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology, 25*(2), 109–125. https://doi.org/10.1057/jit.2010.6

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems, 54*(1), 471–481. https://doi.org/10.1016/j.dss.2012.06.010

Lin, C.-H., Yen, H. R., & Chuang, S.-C. (2006). The effects of emotion and need for cognition on consumer choice involving risk. *Marketing Letters, 17*(1), 47–60.

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. *European Journal of Information Systems, 26*(6), 546–563.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly, 35*(2), 293–334. https://doi.org/10.2307/23044045

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*: Sage.

Milne, G. R., & Boza, M.-E. (1999). Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing, 13*(1), 5–24. https://doi.org/10.1002/(SICI)1520-6653(199924)13:1<5::AID-DIR2>3.0.CO;2-9

Peter, J. P., & Ryan, M. J. (1976). An investigation of perceived risk at the brand level. *Journal of Marketing Research, 13*(2), 184–188. https://doi.org/10.1177/002224377601300210

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879.

Porter, M. E., & Heppelmann, J. E. (2014). How smart, connected products are transforming competition. *Harvard Business Review, 92*(11), 64–88.

Sagiv, L., Amit, A., Ein-Gar, D., & Arieli, S. (2014). Not all great minds think alike: Systematic and intuitive cognitive styles.

Journal of Personality, 82(5), 402–417. https://doi.org/10.1111/jopy.12071

Shiloh, S., Salton, E., & Sharabi, D. (2002). Individual differences in rational and intuitive thinking styles as predictors of heuristic responses and framing effects. *Personality and Individual Differences, 32*(3), 415–429. https://doi.org/10.1016/S0191-8869(01)00034-4

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly, 167–196*. https://doi.org/10.2307/249477

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly, 989–1015*. https://doi.org/10.2307/41409970

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology, 68*(3), 459. https://doi.org/10.1037/0021-9010.68.3.459

Taylor, J. W. (1974). The role of risk in consumer behavior: A comprehensive and operational theory of risk taking in consumer behavior. *Journal of Marketing, 38*(2), 54–60. https://doi.org/10.1177/002224297403800211

Trepte, S., Scharkow, M., & Dienlin, T. (2020). The privacy calculus contextualized: The influence of affordances. *Computers in Human Behavior, 104*, 106115. https://doi.org/10.1016/j.chb.2019.08.022

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems, 17*(5), 328–376.

Westin, A. F. (1967). *Privacy and freedom Atheneum. New York, 7*, 431–453.

Wu, C. H., Parker, S. K., & De Jong, J. P. (2014). Need for cognition as an antecedent of individual innovation behavior. *Journal of Management, 40*(6), 1511–1534. https://doi.org/10.1177/0149206311429862

Xu, H., Dinev, T., Smith, H. J., Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *Proceedings of the International Conference on Information Systems (ICIS),* 6.