Privacy Risk Perceptions in the Connected Car Context

Nils Koester, Patrick Cichy, David Antons, Torsten Oliver Salge
RWTH Aachen University, Germany
{nils.koester; cichy; antons; salge}@time.rwth-aachen.de

Abstract

Connected car services are rapidly diffusing as they promise to significantly enhance the overall driving experience. Because they rely on the collection and exploitation of car data, however, such services are associated with significant privacy risks. Following guidelines on contextualized theorizing, this paper examines how individuals perceive these risks and how their privacy risk perceptions in turn influence their decision-making, i.e., their willingness to share car data with the car manufacturer or other service providers. We conducted a multi-method study, including interviews and a survey in Germany. We found that individuals' level of perceived privacy risk is determined by their evaluation of the general likelihood of IS-specific threats and the belief of personal exposure to such threats. Two cognitive factors, need for cognition and institutional trust, are found to moderate the effect that perceived privacy risk has on individuals' willingness to share car data in exchange for connected car services.

1. Introduction

Connected car services promise to significantly enhance the driving experience. Smart parking services help to easily find and book vacant parking spots, telematic insurance tariffs grant discounts for cautious driving and real-time feedback on one's own driving style enhances eco-friendly driving. However, connected car services crucially rely on processing the data that vehicles' on-board sensors and GPS modules generate (such as vehicle position, acceleration and breaking data, radar data). Since such car data allow for various inferences about drivers, the collection, storage and processing of such digital exhaust has implications for individuals' privacy, meaning the control an individual has over information about oneself [32, 40]. Connected cars can hence be considered as privacy-invasive information systems (IS) [12]. Established privacy-calculus models suggest that individuals weigh risks against benefits when deciding about whether they want to adopt such IS and share personal data with other parties [38]. However, the process of how individuals actually evaluate relevant contextual factors in forming their risk perceptions has only received very little attention from privacy scholars. It is hence not well understood how individuals – confronted with a distinctive privacy-invasive IS and its specifics like technical features, usage context, involved stakeholders, etc. – form privacy risk perceptions and ho w they anticipate these in their decision-making.

Addressing this research gap appears particularly timely, as the wave of novel privacy-invasive IS, namely Internet of Things (IoT) devices or smart products, is already reaching virtually all areas of private and professional life [29]. The associated privacy risks that such products entail are expected to be more profound and far-reaching than what consumers had to deal with in extant technological contexts. The connected car in particular is associated with a large variety of privacy risks, which can even take the form of "life-threatening" breaches, like hacking attacks that deactivate a cars' braking system [29]. In response to this clear need for research, this paper sheds light on the formation and behavioral consequences of privacy risks in the context of connected cars. Only when the formation of privacy risks is understood as a highly context-specific, multifaceted assessment, scholars and service providers will be able to better understand customers' data sharing decisions and identify opportunities for service improvement [26]. Given the novelty of our study context, we adopted a context-sensitive approach in our theorizing [24]. With the goal to generate insights of high practical relevance, this approach suggests paying close attention to characteristics of the IS artifact as well as to its usage context and integrate these in the process of theorizing.

The anticipation of privacy risks has frequently been shown to reduce individuals' intention to share personal data [27, 28, 42]. While privacy is being defined as a highly context-sensitive concept, common measurements of how its loss is perceived by individuals are pictured as abstract and unidimensional [25].

URI: https://hdl.handle.net/10125/71153
978-0-9981331-4-0

Privacy risks and privacy concerns as the most common conceptualizations in this regard [38], usually neglect the specific manifestations of privacy risks in the respective context. This shortcoming limits the contribution extant quantitative examinations have in explaining the formation and consequences of privacy risks [25].

Different IS will be more or less likely to cause specific negative consequences that are related to the loss of control over the collection and use of personal data. Such negative consequences depend not only on the technical features of an IS, but also other aspects such as users' degrees of freedom in deciding which information to disclose, the involved stakeholders and the legal safeguards in place. These determinants for privacy risk will be different for connected cars than, for instance, in the context of social media applications [28]: In the context of connected cars, social consequences might be less likely, as the spectrum of delicate private information is more limited compared to social networks and as it seems improbable that car manufacturers have an interest in exposing their customers, for instance, as poor drivers. On the other hand, users of connected cars might be more alarmed of physical consequences, as hackers could manipulate vehicle functions to harm their targets [29].

Our work extends prior literature in at least three ways. First, we conduct rigorously contextualized research in the novel and highly relevant context of connected cars. Second, we provide an integrative perspective on privacy risk perceptions as an individual's assessment of two components: Perceptions of IS-specific threats that might occur to users of the IS in general and their perceived level of personal exposure to such threats. Third, we conduct a context-specific investigation of the cognitive factors influencing the role of privacy risk perceptions in the data sharing decision. We conduct our empirical work in two phases: First, we develop a robust measure for perceived connected car threats in seven dimensions (physical, social, resource-related, psychological, prosecution-related, career-related and freedom-related risks; [25]) and identify further contextual factors of relevance. We draw on the rich data from 33 context-immersive interviews we conducted with car drivers. Second, we then test our hypotheses around the formation and behavioral consequences of privacy risk perceptions, based on data collected through a large-scale online survey among car drivers (n = 791).

2. Conceptual Background

Risk perceptions are assumed a key determinant of consumers' decision making [15]. In general, risk is commonly constructed of two elements: The severity of negative consequences and the likelihood of their occurrence [14]. As risk can hardly be captured objectively, empirical studies predominantly rely on perceived risk, as consumers personal belief regarding risks based on the information available to them [15].

Services that require individuals to disclose personal information pose potential threats to the user's information privacy. Negative consequences can arise through the loss of control over personal data [30]. Two basic constructs have emerged to measure negative consequences associated with data sharing (privacy concerns and privacy risks), which are most commonly used in one of their many variations in research on privacy [38].

Established measurements of privacy concerns focus on individuals' concerns of how organizations handle their data [26]. The CFIP scale, for instance, captures individuals' concerns that privacy-invasive practices (collection, errors in processing as well as unauthorized access or unintended use of personal data) affect them negatively. These concerns entail an emotional, normative notion, as they reflect what "bothers" an individual and what "companies should" do when handling personal data [39]. Privacy concerns thereby serve as a proxy for privacy itself [2] and are often considered as individuals dispositional belief regarding privacy, referring to their tendency to worry about information privacy that is rather consistent across different contexts [30].

In parallel, conceptualizations of privacy risk have emerged in literature. In contrast to privacy concerns, they try to capture an individual's expectations of the consequences of privacy-invasive practices for them. Two categories of conceptualizations can be identified: While several studies define privacy risks as an individual's expectations of other parties behaving opportunistically as they receive access to personal information [44] others conceptualize privacy risks as an individual's expectations of potential disadvantages associated with data disclosure [13, 30, 38]. Opposed to privacy concerns as a more trait-like construct [2], several studies have considered privacy risks a more situation-specific assessment that can override dispositional attitudes [30].

In literature, this distinction of the prevalent concepts privacy concerns and privacy risks is often blurred and their positioning in research models is ambiguous: Many studies use the terms synonymously [5]. More broadly, privacy is often seen as an end in itself rather than a means to avoid negative consequences associated with collection and misuse of data in a specific context. What is more, both privacy risks and privacy concerns are often measured as an individual's "gut feeling" whether a service or medium is

adverse to their privacy, without capturing why a potential limitation of privacy is perceived risky. In other words, these conceptualizations remain "unidimensional and fairly abstract" [25], as they assume that individuals feel negatively impacted by restrictions to privacy, but remain unclear, by which exact consequences of privacy-invasive practices they are – or expect to be – affected. Calling for a context-specific and multidimensional investigation of privacy risks, Karwatzki et al. [25] propose to consider seven dimensions of risks (physical, social, resource-related, psychological, prosecution-related, career-related and freedom-related risks) caused by privacy-invasive practices.

Several studies have outlined specific negative consequences of different privacy-invasive IS: Unintended use of customer information in direct marketing can entail psychological risks, as it violates the consumer's basic need for fairness [10]. In ride-hailing services like "Uber", information on speed and location may be used to penalize drivers if they do not follow the app's instructions [32], reflecting career-related risks. In online social networks, personal information shared can be exploited through commercial agents, be used by employers to generate insights on prospective employees, or even be abused by stalkers [28], reflecting financial, career- and freedom-related risks. Information collected through smart health trackers may result in financial and social risks for users [26], if, for instance, their unhealthy habits are revealed and health insurances shift them to more expensive tariffs. These examples underline that the negative consequences arising from other parties' access to individuals' personal data are highly context-specific, as the likelihood of the different dimensions will vary for different IS.

As individuals build personal perceptions of risk inherent to a transaction based on the information available to them [33], we propose to investigate perceived privacy risk as an assessment of two components: The general likelihood of negative consequences specific to a privacy-invasive IS – in our case, potential connected car threats they perceive – and their personal exposure to these threats, reflecting the severity of negative consequences.

3. Hypotheses

3.1. The formation of privacy risk perceptions based on perceived connected car threats and chronic prevention focus

As widely tested and established in literature, we expect individuals to be less willing to share car data in exchange for a connected car service if perceived privacy risks are high. Hence, we propose the following baseline hypothesis:

H0: *Perceived privacy risk will be negatively associated with intention to share data*.

We expect perceived privacy risk to be a function of the specific negative outcomes of data sharing that individuals anticipate in a specific IS context [26]. As individuals decide whether to share car data in exchange for a connected car service, they will evaluate the likelihood of negative consequences, as well as the form that those negative consequences could take, in relation to factors like physical safety, social status, and freedom [25]. While the dimensions affected by privacy invasion may be similar to other contexts, the exact manifestations of negative consequences and their likelihood of occurrence will be distinctive for connected cars, given their specifics such as technical features, data types, usage context, involved stakeholders, and so on. In particular, we see three main reasons, why the context of connected cars as an IoT application may differ a lot from extant technology contexts privacy has been investigated in: Connected cars (1) generate data of unparalleled amount and specificity, (2) permeate both the virtual and the physical space, and, (3) reflect an IS context highly regulated and characterized by a broad range of different situations and implications of usage.

It was found [9] that individuals associate concrete negative consequences with connected cars – such as unwanted use of data for commercials by car manufacturers, feelings of surveillance, and disadvantages in the settlement of accident claims with car rentals or insurers when their car data was analyzed – and found that these were reasons why potential users were reluctant to share their driving data. We expect that the more strongly individuals believe that negative outcomes may arise from access to users' personal data [25] (here: from connected cars), the more they worry that a loss will result from their sharing of such data [30]. Thus:

H1: *Perceived connected car threats will be positively associated with perceived privacy risk.*

While perceived connected car threats reflect the perceived nature of privacy risks in our context, we argue that an individual's chronic prevention focus reflects the perceived personal exposure to contextual privacy risks. Compared to other privacy-invasive IS, the context of connected cars is characterized by a dense network of rules. For instance, whereas users of smartphones are relatively unconstrained in their activities, car drivers need to comply with traffic regulations such as speed limits, as well as with the manufacturer’s maintenance instructions if they want to maintain warranty protection. The extent to which

drivers comply with relevant rules is structurally different across individuals, as regulatory focus theory postulates [19]: Individuals assess choices based on potential gains and losses, as well as based on potential "nongains" and "nonlosses," meaning the absence of positive and negative outcomes. Individuals can be characterized by their chronic regulatory focus, i.e., their general tendency to be more or less promotion- or prevention focused [23]. Individuals that are generally at the promotion-focused end of the spectrum 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, chronically prevention-focused individuals are highly vigilant and try to behave safely to minimize negative outcomes [7]. In other words, individuals with a high prevention focus are often found to have a lower propensity to risk losses [17] and are more willing to forego opportunities, i.e., to accept nongains. Correspondingly, if was found [19] that prevention-focused individuals are less likely to engage in rule-breaking driving behavior such as speeding. Put differently, driving safely and sticking to the rules helps prevention-focused drivers to fulfill their desire to avoid losses. While these drivers may lose out on travel speed and driving pleasure, i.e., experience nongains, they are content to do so in order to reduce the possibility of accidents as well as financial and legal problems. Building on this point, we argue that an individual's chronic position on the spectrum between prevention focus and promotion focus is determinant to that individual's perceived privacy risk in the context of connected cars. The connected car, constantly collecting and transmitting driving data, may provide car manufacturers, service providers, or even law enforcement authorities with unprecedented means to track compliance with rules, and, in turn, to detect rule-breaking. The degree to which drivers consider negative consequences from sharing car data as severe should thus be affected by their level of prevention focus. As car drivers with high prevention focus are more likely to obey traffic rules and maintenance instructions, they might view the disclosure of their driving style and car handling as less threating than less prevention-focused drivers, who are more likely to engage in traffic offenses such as speeding or to treat their car carelessly. Hence, we propose:

H2: *Chronic prevention focus will be negatively associated with perceived privacy risk.*

2.2. The moderating role of need for cognition and institutional trust

We further expect the negative association between perceived privacy risk and intention to share car data to be moderated by two cognitive factors, need for cognition and institutional trust.

Previous research [27] has investigated the impact of different thinking styles on individuals' privacy risk perceptions and data sharing decisions. Thinking styles describe individual preferences for either experiential thinking or rational thinking, which guide the deliberation and depth of information processing [37]. Individuals with a high need for cognition prefer rational thinking, associated with a more thorough and intensive processing of information compared to individuals with a high faith into intuition, reflecting a preference for experiential thinking [16]. For instance, individuals with a high need for cognition were found to perform better at analytical tasks and to show a higher need for security and conformity [36]. In privacy research [27], evidence was found that individuals with a high need for cognition perceive higher privacy risks due to a more thorough assessment. Building on these findings, but embedding the construct in a contextualized research model, we consider need for cognition as a moderator of privacy risk perceptions rather than an antecedent. As the consideration of privacy risks is a complex task, it is plausible to expect that individuals high in need for cognition more strongly rely on their privacy risk perceptions and are less likely to let their disclosure decisions be diluted by more superficial aspects such as heuristics and biases. We expect drivers with a high need for cognition to attach more weight to their perceptions of privacy risk when performing the privacy calculus in the decision whether to share data in exchange for a connected car service. Hence, we propose:

H3: *The association between perceived privacy risk and intention to share data will be moderated by need for cognition; this means, if need for cognition is high, the negative effect of perceived privacy risk on intention to share car data will be higher as well.*

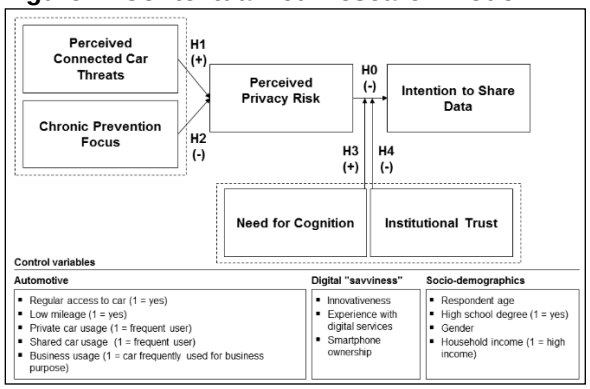
On the other hand, several studies have found evidence for trust as a factor mitigating the effect of perceived privacy risks in the privacy calculus [4, 30]. In privacy research, trust is considered a belief positively influencing an individual's willingness to share personal data, as it embodies the expectation that another actor will not behave opportunistically [38]. The exact positioning of trust and its role in the privacy calculus have been inconsistent across extant privacy studies [38]. In the basic privacy calculus, trust is conceptualized as a benefit dimension, impacting intentions to disclose data independently of the cost dimension [3]. We, however, argue that trust is rather affecting an individual's willingness to accept risk [41] than impacting risk perceptions directly. Trust building has been identified as an important managerial strategy to in-

crease user's willingness to use privacy-invasive services [9], which is potentially more effective than reducing perceived privacy risks per se [9] and more practical to address by service providers. While some work [9, 17] has investigated the impact of relational trust towards the data-requesting stakeholder on risk perceptions, we follow the stronger argumentation of several studies [27, 28] that measured institutional trust as a general tendency towards confidence in a data-collecting institution or medium [27]. We suggest that individuals, trying to reduce cognitive complexity of the data sharing decision, rely on this general tendency towards a stakeholder group rather than to assess the specific provider's relational trustworthiness. 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 working together to arrive at a critical mass of users. If drivers assume that established car manufacturers have taken the respective measures to prevent negative consequences for their customers, for instance, through secure data transmission or anonymization, they will assign less weight to their privacy risk perceptions in the disclosure decision. We therefore formulate:

H4: *The association between perceived privacy risk and intention to share data will be moderated by institutional trust; this means, if institutional trust is high, the negative effect of perceived privacy risk on intention to disclose car data will be attenuated.*

Figure 1 shows our research model.

Figure 1: Contextualized Research Model.



4. Methods

We conducted our empirical work in two phases: Before testing our hypotheses through a large-scale online survey, we conducted a qualitative pre-study (semi-structured interviews) We did so to further enhance contextualization of our research model, closely following respective guidelines [24]. As we contextualized the established privacy calculus perspective through adding further core constructs (chronic prevention focus and need for cognition; contextualization level 1) and a contextual moderator (institutional trust towards car manufacturers; contextualization level 2b), the objectives of our pre-study have been the threefold: First, we wished to investigate whether the dimensions of privacy risk put forward [26] do hold in the IoT context and the connected car setting in particular. Second, we aimed to develop a robust measure for perceived connected car threats. Lastly, we sought to identify context-specific control variables (contextualization level 2a, [24]) that might impact the intention to share car data.

4.1. Pre-study: Developing and Enhancing the Contextualized Research Model

Design and procedure. In our interview setting, we went beyond the mere hypothetical, scenario-based approach which is usually applied by privacy scholars [3, 26]. To enhance the validity of our qualitative examination, we placed participants on the driver's seat of a connected car and interviewed them after showcasing the connected car services. We recruited 33 car drivers in Germany (age: min = 19 years, max = 83 years, M = 36.3 years, SD = 17.7; gender: M = 52% male; car usage: 49% frequent drivers). After a live demonstration of the connected car, we asked respondents to elaborate on, for example, their attitude towards connected cars, what they like and dislike about the demonstrated services, and their ideas on how to improve connected car functionalities and services.

Data analysis. A detailed discussion of the data analysis goes beyond the scope of this paper and can be provided by the authors upon request. We conducted a content analysis of the interview material to derive categories and subcategories of negative consequences individuals associated with sharing car data. We compared our categories and subcategories to extant privacy research. Our categories corresponded well to the seven privacy risk dimensions proposed by Karwatzki et al. [25] whose multidimensional privacy risk scale was developed through consumer research. Furthermore, our subcategories closely matched the negative consequences associated with connected cars that Cichy [8] identified. We decided to adopt their categorizations to arrive at an integrated system of privacy risk dimensions and specific negative consequences relevant in the connected car context.

Findings. Table 1 presents the perceived connected car threats reflected in our interviews. We could detect all of the seven privacy risk dimensions

put forward [26], namely psychological, social, freedom-related, prosecution-related, financial, career-related, and physical risks in our interview data as well. What is more, we were able to reproduce findings of [8] on the various connected car-specific threats even though our interview setting and design differed significantly. This increases the confidence in the validity of our final set of connected car-specific threats that we use to create a measuring instrument. Collectively, our pre-study extends and integrates extant research in three ways: First, we line out exact, IS-specific threats that constitute the multiple dimensions of privacy risks. Second, we develop the first holistic categorization linking perceived IS-specific threats with privacy risk dimensions and privacy-invasive practices, contributing to a precise understanding of privacy risks. Third, we are able to validate the privacy risks dimensions put forward [26] and the negative consequences associated with connected cars [8] identified in a more real-life investigation setting. Beyond perceived connected car threats, the interviews indicated a number of contextual factors that might impact the intention to disclose car data, like driver's age, smartphone ownership or mobility habits. Based on this, we derived several covariates specific to the context of connected cars we included as control variables in our research model (see figure 1).

Table 1: Perceived connected car threats reflected in our Interviews (n = 33).

Priv. Risk Dimension [25]	**Perceived connected car threat [8]**	**Priv. invasive practice [39]**	**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)*
	Distraction, feeling overwhelmed (8/33)	Collection	*"But this is distracting, as I realized. You are permanently thinking: 'Oh, OK, what do I need to do differently?'" (13.2)*
Physical	Criminals identify vulnerabilities (8/33)	Collection	*"Okay, this car is empty, or Mrs. XY is driving alone through the forest" (7.3)*
	Manipulation of vehicle functions through hackers (6/33)	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 (2/33)	Collection	*"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 (2/33)	Errors	*"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 (8/33)	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)*
	Enforced repair jobs (4/33)	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 (2/33)	Secondary use	*"Maybe I will be told that my driving style caused more wear and tear and thus they reject goodwill claims" (16.3)*
Freedom-related	Unsolicited ads (5/33)	Secondary use	*"You will be bombarded with ads, as they know which shops you visit, etc." (7.4)*
	Use of data for un-intended purposes (5/33)	Secondary use	*"I wouldn't want that my data is sold to external providers, so they can adjust their sales activities" (8.5)*
	Data leaks (3/33)	Unauthorized access	*"The more companies possess my data, the more vulnerable is my data to […] hacker attacks" (5.6)*
Prosecution-related	Automatized prosecution of traffic offenses (3/33)	Secondary use	*"I'd be concerned that someday all manufacturers are connected to the police […] and you automatically receive tickets" (33.3)*
	Optimization of radar control position (2/33)	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)*
Career-related	Disadvantages when performing driving jobs (2/33)	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)*

4.2. Main study: Testing the refined contextualized research model

Design and procedure. For our 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.

The questionnaire consisted of three 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 (SmartParking, EcoDriver, 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. We then captured our constructs. For our final sample, we excluded participants who showed unreasonable completion times or failed an attention check as well as respondents under 18 years. This resulted in an overall

sample size of 791 individuals, (min = 18; max = 69; SD = 12.51; female = 55%, mean age = 28 years, high school degree = 86%).

Measurements. Figure 1 shows all main and control variables included. Perceived connected car threats were measured using the scale we developed as part of the qualitative pre-study. All other main variables were captured through established measures from extant studies, as both shown in the appendix. As our research relies on self-reported data, it is exposed to a potential common method bias [41]. 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 [34], we found only marginal differences (i.e., a maximum delta of 0.02 between estimates) and gained confidence in the robustness of our data.

Findings. To test our hypotheses, we performed a multiple moderation regression analysis based on ordinary least squares path analysis [21] with heteroskedasticity-consistent standard errors (HC3; [22]). Collectively, all hypotheses are supported: Perceived connected car threats and chronic prevention focus are antecedents of perceived privacy risk (positive, respectively negative effect); perceived privacy risk is negatively associated with intention to share data, with this association being moderated by need for cognition (positive effect) and institutional trust (negative effect). Table 2 shows our regression results.

Table 2: Results from Multiple Moderation Regression Analysis.

	Dependent variables - B (SE HC3)					
Independent variables	**Perc. Privacy Risk**			**Intention to Disclose**		
Main effects						
Connected Car Threats	0.787	***	(0.047)	0.070		(0.075)
Chr. Prevention Focus	-0.142	***	(0.048)	0.057		(0.063)
Perc. Privacy Risk				-0.654	***	(0.051)
Institutional Trust				-0.050		(0.059)
Need for Cognition				-0.156	**	(0.051)
Interactions						
PR X Trust				0.063	**	(0.059)
PR X Need for Cogn.				-0.163	***	(0.122)
Control variables						
Reg. Access to Car	-0.131		(0.156)	0.335	*	(0.187)
Low Mileage	-0.010		(0.147)	0.053		(0.174)
Private Car Usage	-0.272	**	(0.131)	0.023		(0.177)
Car Sharing Usage	0.150		(1.177)	-0.037		(0.907)
Business Usage	0.253		(0.126)	-0.208		(0.173)
Innovativeness	-0.121	***	(0.046)	0.255	***	(0.060)
Digital Experience	0.041		(0.067)	-0.150	*	(0.086)
Smartphone Owner	-0.803	*	(0.415)	0.193		(0.896)
Age	0.008	*	(0.005)	-0.001		(0.006)
High School Degree	0.170		(0.155)	0.126		(0.190)
Gender	-0.087		(0.100)	0.312	**	(0.131)
High Income	0.025		(0.146)	-0.125		(0.193)
Constant	-2.183	***	(0.623)	2.258	**	(1.082)
R-squared	0.292			0.324		
F-squared	0.412			0.479		

Notes. Total observations = 791. Unstandardized estimates from Ordinary Least Squares (OLS) models. Heteroskedasticity-consistent standard error (HC3, [22]) in parentheses. 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

5. Conclusion and implications

5.1. Implications for research

The objective of this paper was to paint a nuanced picture of how individuals form privacy risk perceptions when deciding whether to share car data in exchange for a connected car service and how these perceptions affect their data sharing decisions. We presented arguments and empirical evidence suggesting that individuals base their privacy risk perceptions on an assessment of two components: Perceptions of IS-specific threats that might occur to users of the IS in general and their perceived level of personal exposure to such threats. This reflects the notion of likelihood and severity of negative consequences as determinants for risk perception that has been established across different contexts and disciplines. With the exact negative consequences and their likelihood being highly context-specific, we identify perceived connected car threats as a contextual antecedent increasing the level of perceived privacy risk. On the other hand, we find an individual's chronic prevention focus to decrease the level of perceived privacy risk, as individuals with a high tendency to comply to rules perceive a lower personal exposure to connected car-specific threats. Furthermore, our findings picture data sharing decisions as cognitively complex processes: Individuals with a higher need for cognition consider their privacy risk perceptions more strongly in the privacy decision. A high institutional trust towards car manufacturers, on the other hand, reduces the effect of privacy risk perceptions on data sharing intentions.

Our findings help retracing how exactly individuals, confronted with a distinctive privacy-invasive IS and its specifics, form privacy risk perceptions and how they consider these in the decision whether to share data. The findings pose several contextual, conceptual and methodological implications. First, we respond to the call for context-specific theorizing in IS research [24] and generated rich and relevant insights as well as applicable advice for practitioners. We contribute to expanding the limits of privacy research through exploring one of the emerging IoT contexts. As privacy risks can even take the form of "life-threatening" breaches affecting the whole society (Lowry et al. 2017), our work underlines the important role of physical and prosecution-related threats in privacy risk perceptions that distinguishes connected cars from established contexts for privacy research like direct marketing, online shopping and social networks [10, 30,

28]. This way, connected cars blur the lines between the commonly distinctive concepts of information and physical privacy [38]. Research in other IoT contexts such as smart home should further investigate this convergence. Second, we make several contributions to extant conceptual models of data sharing decisions. Our study addressed the critique of prevalent conceptualizations of privacy risk being abstract and unidimensional [26], by identifying the specific threats caused by the privacy-invasive practices of connected cars. Incorporating IS-specific negative consequences as an antecedent of privacy risk perceptions rather than as scale of perceived privacy risk itself thereby remains connectivity to extant research and comparability across IS contexts. Decomposing privacy risk perceptions into an assessment of likelihood and severity of negative consequences helps dismantling the ambiguous and vague use of conceptualizations of privacy risks [20]. It further enhances the compatibility of privacy research to other areas investigating risk perceptions in consumer behavior, as the notion of likelihood and severity dimension, although well established in research on risks, has not been followed consistently by extant research on privacy risks. Our study is a case in point that research should conceptualize privacy risk perceptions as an outcome of dedicated, IS-specific threats and an individual's subjective level of exposure to these risks, rather than considering privacy risks as fears of vague disadvantages. Further, our findings substantiate the work on regulatory focus, thinking style, and institutional trust in privacy literature and provide guidance for further use of these concepts in contextualized research. While extant research [6] has focused on situational prevention focus as a moderator of privacy risk perceptions, we conceptualize chronic prevention focus as an adequate proxy for general compliance to rules and norms, reflecting an individual's personal exposure to negative consequences of privacy-invasive practices. While prior research [27] considers need for cognition a factor increasing situational privacy risk perceptions per se, we find support for the moderating role of need for cognition, increasing the effect of privacy risk perceptions. On the other side, our evidence suggests institutional trust as a moderator that attenuates the effect of privacy risk perceptions. In novel IoT contexts such as connected cars, we advocate to implement institutional trust as a moderator of privacy risk perceptions, as individuals are unlikely to have relational experience with specific service providers' trustworthiness. More fundamentally, our investigation of institutional trust and need for cognition contributes to the growing critique of the privacy calculus and its core assumption of individuals as rational agents [2]. Our study adds to the increasing stream of literature that integrates aspects from behavioral economics better explain paradoxical behaviors in privacy decisions [1]. Third, in terms of methodological contributions, our pre-study confirmed the dimensions of privacy risk put forward [26] in another IoT context and validated an exhaustive set of perceived connected car threats from extant literature [8] in a realistic connected car setting, providing respondents with a live demonstration rather than a hypothetical scenario. By doing so, we created a robust measure that is readily available for further studies investigating the highly relevant connected car context and that can also inspire measures for perceived threats in other IS contexts

5.2. Implications for practice and policy

Our research responds to calls to address issues in privacy that are unresolved and controversial in practice rather than spotting gaps in prior literature [29, 35]. Privacy risk perceptions are a decision-making factor for customers that service providers can actively alter. The perceived connected car threats outlined in our study serve as actionable advice, which dimensions to address to reduce customers' hesitance towards sharing car data. Our findings point at the high prevalence of concerns regarding negative consequences for one's physical safety , for instance, through criminals identifying daily routines and hacker attacks. Also, individuals are frequently concerned of disadvantages through secondary use of data, revealing their traffic offences and improper handling of the vehicle. Car manufacturers could mitigate these risk perceptions, if they establish and communicate privacy policies that, for instance, explicitly exclude provision of data to prosecution authorities.

Notably, not all the risk perceptions that individuals may have are fully reasonable, as measures like legal safeguards and cybersecurity measures may reduce the probability of certain consequences to a minimum. For practitioners, it may be especially insightful to review the delta between perceived privacy risk of users and the actual privacy risks […] to learn which risks are overestimated and which are underestimated by users. Correspondingly, we show that policies play a key 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.

6. Limitations and future research

Our study is subject to several limitations. Although widely used in IS research, using a hypothetical

scenario in our survey rather than measuring actual usage behavior is a limitation of our study. We partly addressed this in our pre-study by using a realistic connected car setting with live demonstration rather than a purely hypothetical scenario. We also point out that our sample is not representative of the population in terms of age and education level. A further constraint of our study lies in the geographic context of Germany. As privacy norms and risk perceptions deviate across different geographies and cultural dimensions might interplay with regulatory focus [6], we explicitly encourage researchers to conduct replication studies in other countries. Compatibility to investigation of perceived risk in other domains could be increased, if the component of personal severity of the perceived consequences [15] is more deeply embedded in the construct conceptualization.

7. References

[1] Acquisti, A., "Privacy in electronic commerce and the economics of immediate gratification", in Proceedings of the 5th ACM conference on Electronic commerce, 2004.

[2] Alashoor, T., N. Al-Maidani, and I. Al-Jabri, "The Privacy Calculus under Positive and Negative Mood States", 2018.

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

[4] Bansal, G. and D. Gefen, "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online", Decision support systems, 49(2), 2010, pp. 138–150.

[5] Bélanger, F. and R.E. Crossler, "Privacy in the digital age: a review of information privacy research in information systems", MIS quarterly, 2011, pp. 1017–1041.

[6] Brakemeier, H., T. Widjaja, and P. Buxmann, "Calculating with Different Goals in Mind–the Moderating Role of the Regulatory Focus in the Privacy Calculus", 2016.

[7] Chitturi, R., R. Raghunathan, and V. Mahajan, "Delight by design: The role of hedonic versus utilitarian benefits", Journal of marketing, 72(3), 2008, pp. 48–63.

[8] Cichy, P., Essays on Privacy in the Digital Age, Dissertation: RWTH Aachen University, 2017.

[9] Cichy, P., T.-O. Salge, and R. Kohli, "Extending the privacy calculus: the role of psychological ownership", 2014.

[10] Culnan, M.J. and P.K. Armstrong, "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation", Organization science, 10(1), 1999, pp. 104–115.

[11] Diamantopoulus, A. and H. Winklhofer, "Index construction with formative indicators: An alternative to scale development", Journal of Marketing Research, 38, pp. 269-277.

[12] Dinev, T. and P. Hart, "Internet privacy concerns and their antecedents-measurement validity and a regression model", Behaviour & Information Technology, 23(6), 2004, pp. 413–422.

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

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

[15] Dowling, G.R. and R. Staelin, "A model of perceived risk and intended risk-handling activity", Journal of consumer research, 21(1), 1994, pp. 119–134.

[16] Epstein, S., R. Pacini, V. Denes-Raj, and H. Heier, "Individual differences in intuitive–experiential and analytical–rational thinking styles", Journal of personality and social psychology, 71(2), 1996, p. 390.

[17] Gefen, D., I. Benbasat, and P. Pavlou, "A research agenda for trust in online environments", Journal of Management Information Systems, 24(4), 2008, pp. 275–286.

[18] Grant, H. and E.T. Higgins, "Optimism, promotion pride, and prevention pride as predictors of quality of life", Personality and Social Psychology Bulletin, 29(12), 2003, pp. 1521–1532.

[19] Hamstra, M.R.W., J.W. Bolderdijk, and J.L. Veldstra, "Everyday risk taking as a function of regulatory focus", Journal of research in personality, 45(1), 2011, pp. 134–137.

[20] Hauff, S., D. Veit, and V. Tuunainen, "Towards a taxonomy of perceived consequences of privacy-invasive practices", ECIS 2015 proceedings, 2015.

[21] Hayes, A.F., Introduction to mediation, moderation, and conditional process analysis: A regression-based approach, Guilford publications, 2017.

[22] Hayes, A.F. and L. Cai, "Using heteroskedasticity-consistent standard error estimators in OLS regression: An introduction and software implementation", Behavior research methods, 39(4), 2007, pp. 709–722.

[23] Higgins, E.T., "Promotion and prevention: Regulatory focus as a motivational principle", Advances in experimental social psychology, 30, 1998, pp. 1–46.

[24] Hong, W., F.K.Y. Chan, J.Y.L. Thong, L.C. Chasalow, and G. Dhillon, "A framework and guidelines for context-specific theorizing in information systems research", Information Systems Research, 25(1), 2014, pp. 111–136.

[25] Karwatzki, S., M. Trenz, V.K. Tuunainen, and D. Veit, "Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence", European Journal of Information Systems, 26(6), 2017, pp. 688–715.

[26] Karwatzki, S., M. Trenz, and D. Veit, "Yes, firms have my data but what does it matter? measuring privacy risks", ECIS 2018 proceedings, 2018.

[27] Kehr, F., T. Kowatsch, D. Wentzel, and E. Fleisch, "Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus", Information Systems Journal, 25(6), 2015, pp. 607–635.

[28] Krasnova, H., S. Spiekermann, K. Koroleva, and T. Hildebrand, "Online social networks: Why we disclose", Journal of information technology, 25(2), 2010, pp. 109–125.

[29] Lowry, P.B., T. Dinev, and R. Willison, "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), 2017, pp. 546–563.
[30] Malhotra, N.K., S.S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model", Information Systems Research, 15(4), 2004, pp. 336–355.
[31] Möhlmann, M. and L. Zalmanson, "Hands on the wheel: Navigating algorithmic management and Uber drivers' autonomy", ICIS 2017 proceedings, 2017.
[32] Moon, Y, "Intimate exchanges: Using computers to elicit self-disclosure from consumers", Journal of Consumer Research, 26(4), pp. 323-339.
[33] Pavlou, P.A., "Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model", International journal of electronic commerce, 7(3), 2003, pp. 101–134.
[34] Podsakoff, P.M., S.B. MacKenzie, J.-Y. Lee, and N.P. Podsakoff, "Common method biases in behavioral research: a critical review of the literature and recommended remedies", Journal of applied psychology, 88(5), 2003, p. 879.
[35] Rai, A., "Editor's comments: Diversity of design science research", MIS quarterly, 41(1), 2017, pp. iii–xviii.
[36] Sagiv, L., A. Amit, D. Ein-Gar, and S. Arieli, "Not all great minds think alike: Systematic and intuitive cognitive styles", Journal of Personality, 82(5), 2014, pp. 402–417.
[37] Shiloh, S., E. Salton, and D. Sharabi, "Individual differences in rational and intuitive thinking styles as predictors of heuristic responses and framing effects", Personality and Individual Differences, 32(3), 2002, pp. 415–429.
[38] Smith, H.J., T. Dinev, and H. Xu, "Information privacy research: an interdisciplinary review", MIS quarterly, 2011, pp. 989–1015.
[39] Smith, H.J., S.J. Milberg, and S.J. Burke, "Information privacy: measuring individuals' concerns about organizational practices", MIS quarterly, 1996, pp. 167–196.
[40] Stone, E.F., H.G. Gueutal, D.G. Gardner, and S. McClure, "A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations", Journal of applied psychology, 68(3), 1983, p. 459.
[41] Venkatesh, V., J.Y.L. Thong, and X. Xu, "Unified theory of acceptance and use of technology: A synthesis and the road ahead", Journal of the association for Information Systems, 17(5), 2016, pp. 328–376.
[42] Wang, T., T.D. Duong, and C.C. Chen, "Intention to disclose personal information via mobile applications: A privacy calculus perspective", International journal of information management, 36(4), 2016, pp. 531–542.
[43] Westin, A.F., "Privacy and freedom Atheneum", New York, 7, 1967, pp. 431–453.
[44] Wu, Y., "Influence of social context and affect on individuals' implementation of information security safeguards", ICIS 2009 Proceedings, 2009, p. 70.

Appendix: Construct Measures

<table>
<tr><td>A) Perceived Privacy Risk* (adapted from [14]; CA = 0.87; CR = 0.87, AVE = 0.63)</td><td>B) Chronic Prevention Focus* (adapted from [21]; CA = 0.68; CR = 0.80; AVE = 0.53)</td></tr>
<tr><td>C) Institutional Trust* (adapted from [37]; CA = 0.88; CR = 0.88; AVE= 0.72)</td><td>D) Need for Cognition* (adapted from [16]; CA = 0.77; CR = 0.84; AVE = 0.57)</td></tr>
<tr><td colspan="2">E) Perceived Connected Car Threats** (self-developed) How do you assess the likelihood of occurrence of the following scenarios?</td></tr>
<tr><td>[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.</td><td>[Physical risks]
9. 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).
10. Hackers manipulate vehicle functions (e.g., window lifts, breaks).
[Social risks]
11. Drivers are stigmatized as bad drivers.
12. 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]
13. Car manufacturer (mis)use shared driving data for unexpected purposes or resale the data to other companies.
14. Increase of unsolicited advertisement and rebate offerings by car manufacturers.
15. Criminals steal or manipulate driving data (e.g., through data leaks, hacker attacks).</td></tr>
<tr><td colspan="2">Notes. 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. For our novel construct Perceived Connected Car Threats which we specified as an index with formative indicators, common measures for validity and internal consistency are not appropriate [11]. We however found confidence in the adequate validity through bottom-up construction based on our interviews and through comparison to extant studies [8, 26]. A detailed appendix on the construct development process can be provided by the authors upon request.</td></tr>
</table>