Maximizing Smart Charging of EVs: The Impact of Privacy and Money on Data Sharing

Hanna Marxen
SnT - Interdisciplinary centre for security reliability and trust, University of Luxembourg, hanna.marxen@uni.lu

Raviteja Chemudupaty
University of Luxembourg, raviteja.chemudupaty@uni.lu

Gilbert Fridgen
University of Luxembourg, gilbert.fridgen@uni.lu

Tamara Roth
University of Luxembourg, tamara.roth@uni.lu

Maximizing Smart Charging of EVs: The Impact of Privacy and Money on Data Sharing

Completed Research Paper

Hanna Marxen
SnT, University of Luxembourg
Luxembourg, Luxembourg
hanna.marxen@uni.lu

Raviteja Chemudupaty
SnT, University of Luxembourg
Luxembourg, Luxembourg
raviteja.chemudupaty@uni.lu

Gilbert Fridgen
SnT, University of Luxembourg
Luxembourg, Luxembourg
gilbert.fridgen@uni.lu

Tamara Roth
SnT, University of Luxembourg
Luxembourg, Luxembourg
tamara.roth@uni.lu

Abstract

Smart charging has the potential to shift peak load to times of lower demand, which better exploits renewable generation and enhances grid resilience. For increased effectiveness, smart charging requires access to data that consumers might be hesitant to share. To explore which data consumers would share and which factors influence this decision, we adopt the Barth and de Jong's risk-benefit calculation framework to smart charging and conduct an online-survey (n = 479). We find that most respondents who would share charging details with a smart charging application, are ambivalent about location data and would never share calendar details. When presented with concrete monetary rewards, participants lose their initial reservations and would share all data for an amount dependent on the data's sensitivity. Thus, our study contributes to research on the privacy paradox by highlighting the importance of calculations between perceived risks and benefits for the decision to share data.

Keywords: Smart charging, consumer data, data sharing, privacy concerns, monetary incentives

Introduction

The use of electric vehicles (EVs) has increased rapidly in recent years. Governmental incentive schemes and sales bans on combustion vehicles will likely bolster this trend (Shepardson et al., 2021). What appears at first glance to be a big step towards more sustainability also puts tremendous pressure on the energy grid (IEA, 2022). Managing thousands of simultaneous EV charging events combined with regular peaks in electricity consumption and volatility of renewable energy sources (RES) could strain the grid and threaten energy security (Papaefthymiou et al., 2018). However, if EVs are charged in a controlled manner, i.e., through smart charging, they could instead become a flexible asset and support grid stability. Smart charging means that energy providers can optimally adjust the EV charging schedule in response to power system signals (e.g., RES generation) while meeting user requirements (IRENA, 2019).

To fully exploit the flexibility potential of EVs and implement smart charging, it is imperative for energy providers to understand the charging patterns of EVs. Understanding and accurately predicting these charging patterns helps energy providers tailor their services to individual EV users and support grid resilience. Charging patterns typically manifest for different types of data: Historical charging behavior and smartphone location data will help predict future charging behavior. Data linked to a person's schedule (e.g., via a calendar) can be even more accurate and helpful to optimize EV charging. Advances in pattern prediction may further automate smart charging so EV users become less involved.

Despite the advantages of accurate charging pattern prediction, consumers might be reluctant to share their data due to privacy concerns (Aloise-Young et al., 2021; Barth et al., 2019; Smith, 2008; Smith et al., 2011). They fear losing control of who has access to and can use their data (Cichy et al., 2021). At the same time, consumers readily share data in online contexts, such as social media or e-commerce, sometimes forgetting their initial concerns about data privacy (Chakraborty et al., 2013; Kokolakis, 2017). This ambiguous relationship between privacy and data sharing is often termed as the 'privacy paradox' and is a well-researched phenomenon (Buckman et al., 2019; Kim et al., 2019; Wu et al., 2020). Moreover, studies on social-hedonic and financial rewards have indicated that risk-taking behavior, such as excessive private data sharing, depends on the ratio of perceived benefits versus perceived risks (Turel, 2021).

Most privacy paradox studies focus on the active sharing of information with an online service provider. However, the findings of these studies may not be fully applicable in the context of smart charging. Cichy et al. (2021) argue in their research on data sharing for connected cars, which – much like location data sharing for smart charging – relies on IoT devices, that common data sharing reservations in online service contexts may not apply to IoT devices. "IoT devices (1) tend to be 'always on' and generate continuous data streams, (2) give users little or no power to control the data flows, (3) require unrestricted data access to fully function, and (4) invade users' virtual and physical space given the increasingly powerful actuators—components that transform electric impulses into physical actions—they are equipped with" (p. 1864). These four characteristics distinguish data sharing mechanisms of IoT and connected cars from data sharing mechanisms in online contexts, such as social media and e-commerce (Cichy et al., 2021). For example, sharing data on social media or online shopping does not typically require a user's current location or access to their calendars. Thus, smart charging comes with different privacy concerns than social media or online shopping.

Since most observations focus on the privacy paradox in e-commerce and social media interactions, there is a need to investigate factors influencing the readiness to share data in an IoT context, such as smart charging. Although studies have highlighted the importance of sensitive data for smart charging (Bhusal et al., 2021; Habbak et al., 2022), we just found one study that examined whether privacy concerns, perceived risks, and potential environmental benefits influence data sharing with EVs (Alotaibi et al., 2023). The study explored the general data sharing behavior for different EV services. Still, it does not elaborate on the readiness to share data for smart charging nor does it say anything about the sharing behavior of different data types with varying degrees of sensitivity. The study also did not investigate whether people would be more willing to share their personal information when presented with some form of monetary compensation (Hirschprung et al., 2016; Wagner et al., 2018). The relevance of monetary compensation to balance perceived risks is well known from financial economics (e.g., Caraco et al. 1980; Payne et al. 2017), so our study aims to explore its applicability to data sharing with a smart charging application. We therefore asked the following research questions:

RQ1: What data types do individuals intend to share for smart charging?

RQ2: Which factors impact individual's intention to share data with their smart charging application?

RQ3: How much does the monetary incentive need to be for individuals to share different data types for smart charging?

We conducted a large-scale survey to answer our research questions. For RQ1, we explored which data types participants would be most comfortable sharing to enable smart charging. For this evaluation, we included three different types of data (charging history, smartphone location, calendar data). Each of these data types came with varying degrees of sensitivity. To answer RQ2, we used the theoretical framework of Barth and de Jong (2017), commonly applied in privacy paradox research, which integrated key theories on mobile computing. Unlike the thematically related framework of Cichy et al. (2021), the Barth and de Jong (2017) framework specifically focuses on data sharing in mobile computing, making it more suitable for our context. We also explored attitudes towards data sharing and perceived risks and benefits of using the smart charging application, building on theories like foraging and risk sensitivity (Turel, 2021). We additionally assessed data sharing habits and their effect on participants' data sharing intentions. To evaluate the impact of monetary incentives, we introduced an experimental setting to our survey with one experimental and one control group. To answer RQ3, we explored the amount participants would request from the energy provider for sharing data with varying degrees of sensitivity. Answering these research questions contributes to both theory and practice.

Our contributions are three-fold. First, we apply the framework of Barth and de Jong to the context of smart charging. We add to this framework by investigating data sharing behavior for data with varying degrees of sensitivity. Specifically, we look into the differences between moderately and highly sensitive data and how far the framework would still apply. Second, we provide a deeper understanding on the trade-off between perceived risks and benefits by applying a risk-sensitivity and foraging theory perspective. Third, we demonstrate the effect of monetary rewards on data sharing behavior, even for highly sensitive data.

The rest of the paper is structured as follows. The theoretical background elaborates on smart charging and the role of data, Barth and de Jong's (2017) theoretical framework and a short introduction to risk-sensitivity and foraging theory. In the third section, we describe our method, data collection, and analysis. In the fourth section, we present the findings of our SEM and the calculation of monetary incentives. In the fifth section, we critically discuss our findings, elaborate on our theoretical and practical contributions, and outline related limitations. We conclude with a summary of our study.

Theoretical Background

Smart charging and the role of data

Adapting the charging behavior of EVs in response to the power system signals whilst considering the user requirements is known as smart charging (IRENA, 2019). Smart charging algorithms help shift the EV charging process to low-demand periods, drastically reducing the need for additional generation capacities (Pawlowski & Dinther, 2020; Schmidt & Busse, 2013). Moreover, EV charging can be synchronized to the availability of energy from RES to reduce grid imbalances due to generation peaks and simultaneously maximize RES consumption (Eldeeb et al., 2018; van der Meer et al., 2018). To best leverage the potential of smart charging solutions, it is vital to accurately predict the flexibility provided by each EV. Flexibility in the context of smart charging describes the amount of energy that the energy provider can shift until the EV battery has reached the desired percentage within the indicated parking time (Develder et al., 2016; Guthoff et al., 2021; Saxena et al., 2015). Practitioners typically use mobility data (e.g., arrival time, departure time, distance traveled), charging requests (e.g., energy required at the departure time), EV specifications (e.g., battery capacity and maximum charging power) to calculate the flexibility (Daina et al., 2017; Fridgen et al., 2014).

For smart charging solutions to function efficiently, they require bidirectional data exchange between EV users and the energy provider. This data exchange comes with two obstacles: First, regulations, such as the GDPR (General Data Protection Regulations in Europe), require a high degree of user privacy, complicating the collection of relevant data. Second, users are often cautious when sharing sensitive data (Strüker & Kerschbaum, 2012).

There are a variety of technical and sociotechnical measures to overcome these obstacles. Studies on technical measures aim to increase privacy by design without impeding access to (relevant) data (Teng et al., 2022). Examples of such privacy measures are differential privacy (Fernández et al., 2022), homomorphic encryption (Teng et al., 2022), and distributed learning techniques (McMahan et al., 2017). These measures can also be leveraged for smart charging to improve confidence in the data sharing process. They are, however, not subject to this paper.

Sociotechnical measures typically support the acceptance of data sharing. Although sociotechnical measures have already been established in other contexts, they have not been tested for the acceptance of data sharing in smart charging. Monetary incentives are a prominent sociotechnical measure influencing users' intention to share data in various contexts. Thus, we also investigated their effect in our study along with the type of data people would share with the smart charging application and the factors influencing this decision.

We ground our investigations in the rational risk-benefit calculation framework (Barth and Jong, 2017) and make links to IS theories on risk-sensitivity and the privacy paradox. Based on these theories, we derive our hypotheses and research model.

Rational risk-benefit calculation framework (Barth and de Jong, 2017)

Our study is grounded in the theoretical framework of Barth and de Jong (2017), which is related to the privacy paradox, which describes the contradictory behavior of individuals who express concerns about privacy but often share their data freely. Barth and de Jong (2017) aimed to uncover the factors behind this paradox. They summarize and explain theories of private information sharing with mobile apps. They differentiated between rational and biased decision-making theories in the absence or presence of risk factors and consolidated these ideas in a theoretical framework. Barth and de Jong's framework was referred to in different contexts as health technologies (Fox, 2020) and e-commerce (Kolotylo-Kulkarni et al., 2021). Unlike social media and mobile apps, the privacy paradox hasn't been explored in smart charging, so we applied their rational decision-making framework to this context.

According to the rational decision making framework (Barth & de Jong, 2017), individuals choose the option with the greatest benefits. Attitudes towards information disclosure affect context factors and ultimately influence the readiness to disclose certain information. These attitudes can be privacy concerns, general (institutional) trust, or personality traits. Context factors encompass situational factors or individual and environmental characteristics. Individuals weigh perceived risks against perceived benefits, which affects their disclosure intentions and actions. While Barth and de Jong (2017) tie together multiple literature streams to elaborate on risk-benefit calculations, the perspective introduced by risk sensitivity and foraging theory might suit the context of smart charging. These theories include factors such as esteem and self-actualization that may present interesting angles of explanations for our observations in the users' strive to optimize their gains (Turel, 2021).

Risk sensitivity theory and foraging theory in information systems

The assessment of perceived risks and benefits is also at the core of two theories adapted from behavioral biology. Foraging theory suggests that individuals aim to maximize their benefits while considering the dangers of the activities involved in receiving the benefits (Payne et al., 2017; Stephens & Charnov, 1982). They typically base their decision-making on assessing one particular problem, a 'currency' by which they decide between options, and considering external and internal constraints (Stephens & Krebs, 1986).

Risk sensitivity theory (RST) extends foraging theory by adding flexibility to the interplay between internal and external motivators and constraints. Suppose that perceived benefits, for instance, social-hedonic rewards for displaying 'green' behavior in smart charging, outweigh the perceived risks, such as sharing personal data to maximize energy flexibility. In that case, the reward-utility curve may switch from risk averse to risk prone (Mishra & Fiddick, 2012). Thus, people may share sensitive data in high-risk high-reward contexts (Caraco et al., 1980).

Turel (2021) has only recently adapted both theories to analyze technology-mediated dangerous behaviors. More specifically, he explored the role of social-hedonic rewards on risk-taking in social media contexts and found significant overlap with foraging behavior. Such behavior depends on several external and internal context factors that influence the risk proneness and, dependent on their expression, may drive risk-shifting (Cartar, 1991). That is, the relationship between perceived risks and benefits fluctuates, highly dependent on the information provided (Turel, 2021). The level of provided information is also crucial for privacy considerations, especially in the context of smart charging. – where the use of data is unclear for EV users.

Development of hypotheses and research model

In the following section, we describe the development of our hypotheses derived from the literature. Figure 1 illustrates our research model and hypotheses. As noted earlier, attitudes towards disclosure of information play a crucial role in shaping the decision-making context and, consequently on the perception of risks and benefits (Barth & de Jong, 2017). Such attitudes can encompass general privacy awareness and trust towards the provider who manages the smart charging application. People who are generally more concerned about how their data are handled tend to perceive greater risks and have higher levels of risk awareness (Fortes et al., 2017; Van Slyke et al., 2006). Thus, we propose the following hypothesis:

H1a: Privacy awareness is positively related to perceived risks with the smart charging application.

An energy provider typically controls smart charging applications. The level of trust people have in their energy provider can significantly impact their perception of smart charging applications (Utz et al., 2023). Studies conducted in various areas, such as IoT and e-commerce, suggest that lower trust in the service provider leads to greater perceived privacy risks (Kim et al., 2019; Kim et al., 2008). This concept could be applied to smart charging applications since consumers would have a more direct relationship with their energy provider than with other online service providers. Thus, we hypothesize the following:

H1b: Trust in the energy provider is negatively related to perceived risks with the smart charging application.

If people's trust in their energy provider influences the perceived risks of smart charging applications, it can also affect the perceived benefits. Such benefits could encompass the optimal use of sustainable energy, contributing to stable and sustainable grid infrastructure, and reduced charging costs (Brey et al., 2021). Individuals who have built experience-based trust in their energy provider may perceive the potential benefits of the smart charging application more strongly (Utz et al., 2023). In the study by Söllner et al. (2016), trust in the application provider predicted the perceived usefulness of an application. Thus, we formulate the following hypothesis:

H1c: Trust in the energy provider is positively related to perceived benefits with the smart charging application.

Research indicates that prior behavior can be a reliable indicator of future behavior (Ouellette & Wood, 1998). In an experimental setting, Söllner et al. (2022) demonstrated that habitual use of an application positively influences continuous information system (IS) use. Such IS usage habits might also extend to data sharing habits. Barth and de Jong (2017) included this in their model as an antecedent for data sharing. For this reason, we suggest the following hypothesis:

H2: Prior data-sharing habits are positively related to the intention to share data for smart charging.

According to the framework of Barth and de Jong (2017), attitudes influence the intention to share data and resulting data sharing behavior (Theory of Reasoned Action/ Theory of Planned Behavior, Ajzen, 1985; Ajzen and Fishbein, 1980). Data sharing is often considered risky, as some personal data are sensitive. In the context of smart charging, different data types, such as charging history, smartphone location, and calendar data, can help identify behavioral patterns and create user profiles. We want to determine which types of data individuals would share with a smart charging application.

Data sharing decisions typically depend on evaluating risks against potential benefits (Privacy calculus theory, Culnan and Armstrong, 1999). In the context of smart charging, violation of user privacy could be the greatest perceived risks (Bailey & Axsen, 2015), along with the fear that personal data are used for purposes beyond smart charging (Xu et al., 2012). According to risk-benefit calculation theories, such as privacy calculus theory (Culnan & Armstrong, 1999) or risk-sensitivity theory (Mishra & Fiddick, 2012), the perceived risks and benefits of the smart charging application will influence the intention to share data. According to Alotaibi et al. (2023), the privacy calculus is also crucial to explain data sharing with EV services. Based on this, we formulate the following hypotheses:

H3: (H3a) Perceived risks are negatively, and (H3b) perceived benefits are positively related to the intention to share data for smart charging.

The theoretical framework of Barth and Jong (2017) assumes that contextual factors can influence decision making. In this study, we focus on two contextual factors: The desired level of automation of the smart charging application and monetary incentives. Some studies, for instance, Xu et al. (2008), have treated these factors as inherent benefits of data sharing. We did not include automation as a benefit, as it is unclear if it will become the norm. Instead, we explore the desired level of automation as a variable and its effect on the intention to share data.

Resource exchange theory suggests that users are willing to share some of their data in exchange for services (Donnenwerth & Foa, 1974; Foa, 1971). Services can be personalized and automated (Shah, 2015), or come in the form of monetary rewards. However, to increase service automation, the smart charging application requires more data that users who want automation should be willing to share. This assumption is supported by Kim et al. (2019), who found that people share their data for better personalized services without considering privacy risks. Thus, we hypothesize the following.

H4: The desired app automation is positively related to the intention to share data for smart charging.

We consider monetary incentives as both a context factor and a benefit of smart charging. This approach enables us to test how monetary incentives impact data sharing. Previous studies indicated that privacy comes at a cost with different 'price tags' depending on the sensitivity of shared data (Hirschprung et al., 2016) or the context in which the data are shared (Acquisti et al., 2013).

Other immaterial rewards could also play a role, such as increased user convenience or social-hedonic rewards (Turel, 2021). They are, however, difficult to measure in this context and may have different effects on the readiness to share data. Social-hedonic rewards, for instance, could backfire if users' social network criticizes their readiness to share important data for smart charging instead of applauding their contribution to the environment. Thus, we focus primarily on material rewards whose use is established in the literature (Acquisti et al., 2013; Hirschprung et al., 2016). Monetary rewards have also been proven to be effective in related contexts, such as the general acceptance of smart charging (Kramer & Petzoldt, 2022; Wong et al., 2023). They might effectively encourage data sharing (Cichy et al., 2021). We thus propose the following hypothesis:

H5: *Participants who receive monetary incentives have a higher intention to share data for smart charging than participants who do not.*

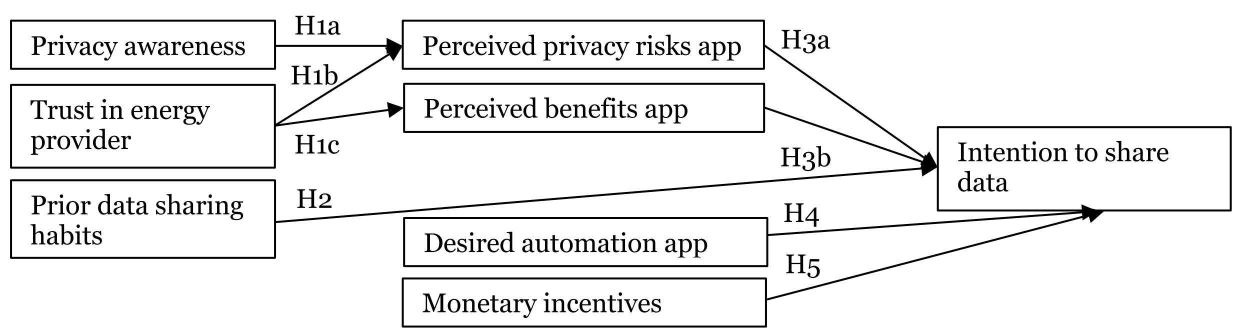

Figure 1. Representation of the hypotheses and research model

Methods

Before conducting the survey, we did a pre-test survey with 20 participants. We included a comment section in the survey to receive impromptu feedback from our pilot group. Feedback primarily concerned the complexity of questions and statements. We changed the survey accordingly and submitted the final draft to the university's ethics committee. After receiving approval from the ethics committee, we started disseminating the survey. Our goal was to get a sample of EV and non-EV users. To achieve this, we distributed the survey widely, including social media and EV user forums, as well as to prolific academics. The survey, which included a questionnaire and a related experiment, was available in English and German. It took about 10-15 minutes to complete the survey.

At the beginning of the survey, we asked participants if they were smartphone users. If they answered "Yes", they received questions about their data sharing habits, such as how many apps they use a month and how many continuously track their location. We measured data sharing habits, as people have many smartphone applications that require location sharing. Additionally, participants rated their familiarity with smart charging on a scale from 1 "not familiar at all" to 7 "extremely familiar". Regardless of their answer, they received a short explanation of smart charging, including potential benefits and requirements. In this way, we wanted to ensure they can make informed decisions when answering our survey.

Participants also received information on how sharing certain data can help the application become more automated and tailored to the charging patterns of users. We assure them that the data would only be shared with the energy provider and not transferred to a third party. Once they finished reading, participants rated the importance of three proposed benefits – facilitating an optimal use of sustainable energy, contributing to a stable energy grid, and reducing charging costs – when using the smart charging application (Brey et al., 2014). They also replied to items on perceived risks during usage (Secondary use of personnel information by Xu et al., 2012) and answered a related attention question. Participants responded to partially adapted scales on privacy awareness (Ponnurangam Kumaraguru & Cranor, 2005), and trust in the energy provider (Döbelt et al., 2015). They indicated their agreement to the respective items on a 7-point Likert scale (1 "Strongly disagree" – 7 – "Strongly agree").

The participants continued with a hypothetical smart charging scenario. They saw a screenshotted mock-up of the smart charging application, which depicted the charging preferences. They selected their preferences by responding to three questions written below the mock-up. These questions inquired about the state of charge (SOC) at arrival, desired SOC at departure, and parking duration. To measure the desired level of automation, participants replied to how often they would want to enter such information manually (1 "before every trip / settings manually" – 9 "once when installing the app / mostly automated").

For the experiment, we randomly assigned participants to the control or experimental group. Participants in the experimental group were notified that they could recover some of their electricity costs if they shared their data with the application. Participants in the control group did not receive this information. After that, we asked all participants which data they would share with the application. They each indicated their willingness to share charging times and preferences, smartphone's location, and full calendar details on a 7-point Likert scale (1 "Strongly disagree" – 7 – "Strongly agree"). In the experimental group, participants also had to imagine that they were frequent drivers with a monthly charging cost of 100 euros. We asked them to indicate how much of the total charging costs they wished to be redeemed for sharing each data type. They could also choose not to share any data type for money. At the end of the survey, participants were informed about the background and purpose of the study and could provide feedback on the survey. To honor their participation, they could sign up for a lottery.

We used structural equation modeling (SEM) to address RQ1 (*What data types do individuals intend to share?*) and answer H1-H5. To calculate the dependent variable, the intention of sharing data, we used a standardized mean of the three data sharing items (composite score). To answer RQ2 (*Which factors impact individual's intention to share data with their smart charging app?*) and RQ3 (*How much does the monetary incentive need to be for individuals to share different data types?*), we analyzed our results descriptively.

Sample

To determine the necessary sample size for the SEM, we used a sample size calculator (Soper, 2022) based on Cohen (2013) and Westland (2010). This analysis indicated that we needed a sample of *n* = 314 (considering a medium effect and a power of 0.8) to calculate our model and detect effects. 501 participants completed the survey. We eliminated participants (*n* = 22) for the following reasons: 1) Participants were not smartphone users (*n* = 10), 2) we detected multivariate outliers according to the Mahalonibis statistical measure (*n* = 12) and/or they answered the survey in less than three minutes or had evident response patterns for different items (*n* = 4). We conducted the analysis with 479 participants.

225 participants (46.97%) were in the experimental group to measure monetary incentives and 254 (53.03%) were in the control group. Most of the participants identified either as men (55.95%), female (40.71%) or diverse (3.34%). They were students (50.31%), worked full time (37.37%), or had other occupations (12.32%). Most of the participants had a master's (44.05%), a bachelor's (21.71%), or different degrees (34.24%). Participants predominantly lived in Luxembourg (50.73%), Germany (33.83%), France (6.26%), Belgium (2.71%), and other countries (6.89%). The three main nationalities were German (31.11%), Luxembourgish (16.70%), and French (6.26%). The mean age was 31.78 (*SD* = 13.03). While 28.18% of participants were EV users and 71.82% were non-EV users, our sample isn't specific to or representative of EV users. Our study primarily examines the willingness to share data for smart charging, irrespective of personal EV experience. Therefore, both EV and non-EV users can answer the survey in the same way.

Results

To answer RQ1, we calculated the mean values of the three data sharing variables for the control and experimental groups. We measured data sharing with a 7-point Likert scale (1 "Strongly disagree" – 7 – "Strongly agree"). Values above 4 indicate that people intend to share these data. The results indicate that the participants are comfortable sharing their charging history and patterns (Exp. Group: *M* = 5.47, *SD* =1.48, *Md* = 6 – "agree", Control group: *M* = 5.65, *SD* = 1.28, *Md* = 6 – "agree") and their location on the smartphone irrespective of monetary incentives (Exp. Group: *M* = 3.92, *SD* = 1.95, *Md* = 4 – "neither agree nor disagree", Control group: *M* = 4.13, *SD* = 1.85, *Md* = 5 – "somewhat agree"). In contrast, participants are not comfortable sharing full calendar details (Exp. Group: *M* = 2.75, *SD* = 1.86, *Md* = 2 – "disagree", Control group: *M* = 2.57, *SD* = 1.77, *Md* = 2 – "disagree").

To test RQ2 and hypotheses 1-5, we calculated a structural equation model, using the package "Lavaan" for "R" (Rosseel, 2012). We checked for the one-dimensionality of the measured items. Each item loaded on its respective underlying concept, and all loadings were significant (see Table 1). The scales' construct reliabilities (CR) were good (Hair, 2017), except for the composite score of intention to share data. Due to variance in the composite score of intention to share data, we additionally calculated three single SEMs with the dependent variables charging history (SEM2), location of the smartphone (SEM3), and calendar details (SEM4).

	Standardized factor loadings			
	SEM1	SEM2	SEM3	SEM4
	Composite score	Historical data	Location data	Calendar data
Privacy awareness	**(CR =.73)**	**(CR = .73)**	**(CR = .73)**	**(CR = .73)**
Consumers have lost all control over how personal information is collected and used by companies. (inverted)*deleted in the analysis				
Most businesses handle the personal information they collect about consumers in a proper and confidential way.	.773	.772	.773	.773
Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.	.740	.740	.740	.740
Trust Energy provider	**(CR =.81)**	**(CR = .81)**	**(CR = .81)**	**(CR = .81)**
My consumption data is being managed securely by my energy supplier.	.652	.652	.651	.650
My energy supplier is billing my consumption correctly.	.757	.757	.757	.756
I can rely on my energy supplier.	.884	.884	.885	.886
Perceived privacy risks with the application	**(CR =.92)**	**(CR = .92)**	**(CR = .92)**	**(CR = .92)**
I am concerned that a smart charging app may use my personal information for other purposes without notifying me or getting my authorization.	.873	.874	.874	.873
When I give personal information to a smart charging app, I am concerned that the app may use it for other purposes.	.910	.908	.910	.910
I am concerned that a smart charging app may share my personal information with other entities without getting my authorization.	.876	.878	.875	.876
Perceived benefits with the application	**(CR =.75)**	**(CR = .76)**	**(CR = .76)**	**(CR = .76)**
Facilitating optimal use of sustainable energy	.837	.822	.846	.859

	Standardized factor loadings			
	SEM1	SEM2	SEM3	SEM4
	Composite score	Historical data	Location data	Calendar data
Facilitating contribution to a stable energy grid	.689	.700	.685	.677
Facilitating reduced charging costs	.597	.604	.592	.586
Intention to share data	**(CR =.63)**			
The location of my smartphone	.726			
My charging times and preferences	.573			
Full details of my calendar (time, subject, location, and other details of all items in your calendar)	.508			

Table 1. Scales of the research model with respective factor loadings and composite reliability (CR). Note: All factor loadings are statistically significant.

The fit of the model with the composite score intention to share data as dependent variable suggests that the model fits the data (χ^2 = 237.598, *df* = 110, *p* < .001, Comparative Fit Index [CFI] = .945, Tucker Lewis Index [TLI] = .934, Root Mean Square Error of Approximation [RMSEA] = .053, Standardized Root Mean Square Residual [SRMR] = .068). Yet, fit indices for the three models with the single data sharing types as dependent variables suggest that the separate models fit even better to the data. The fit indices are as follows: For charging history and patterns as dependent variable (χ^2= 138.965, *df* = 82, *p* < .001, CFI = .972, TLI = .965, RMSEA = .041, SRMR = .057), for the location of the smartphone (χ^2 = 141.326, *df* = 82, *p*< .001, CFI = .971, TLI = .963, RMSEA = .042, SRMR = .059) and for the calendar details (χ^2 = 152.446, *df* = 82, *p* < .001, CFI = .965, TLI = .956, RMSEA = .046, SRMR = .060). Since privacy awareness and trust in the energy provider were highly correlated, we tested this correlation in all four models. Table 2 illustrates the standardized path coefficients and if the hypotheses could be confirmed or rejected for the four models.

	Composite score	Historical data	Location data	Calendar data
	SEM1	SEM2	SEM3	SEM4
	Standardized path coefficients (t-values)			
H1a: Privacy awareness -> Perceived privacy risks app use	.261***	.430***	.430***	.433***
H1b: Trust in energy provider -> Perceived risks app use	-.164**	-.163*	-.164**	-.166**
H1c: Trust in energy provider -> Perceived benefits app use	.261***	.260***	.255***	.247***
H2: Prior location sharing habits -> Intention to share data	.278***	.052 *p* = .089	.153***	.123***
H3a: Perceived privacy risks app use -> Intention to share data	-.457***	-.278***	-.277***	-.336***
H3b: Perceived benefits app use-> Intention to share data	.339***	.379***	.234***	-.025 *p* = .559
H4: Desired automation of the app -> Intention to share data	.047*	-.003 *p* = .872	.055**	.014 *p* = .452
H5: Monetary incentives message -> Intention to share data	-.049 *p* = .614	-.081 *p* = .321	-.083 *p* =.313	.149 *p* = .079
Privacy awareness <-> Trust in energy provider	-.356***	-.356***	-.356***	-.354***

	Composite score	Historical data	Location data	Calendar data
	SEM1	SEM2	SEM3	SEM4
	Standardized path coefficients (t-values)			

Table 2. Empirical evaluation of hypotheses and standardized path coefficients, ****p* **< .05, *****p* **< .01, ******p* **< .001.

To answer RQ3, we grouped the amount of money participants would need to recover from their charging bill to share data. We can interpret the desired amount as percentages since we asked participants to imagine that their electricity bill was 100 euros. Figure 2 illustrates the results. The more sensitive the data is (from charging history to calendar details), the more reluctant participants are to share their data, and the higher the monetary reward participants request. We observed that more than 50% of participants would share their data for money for all three data types,

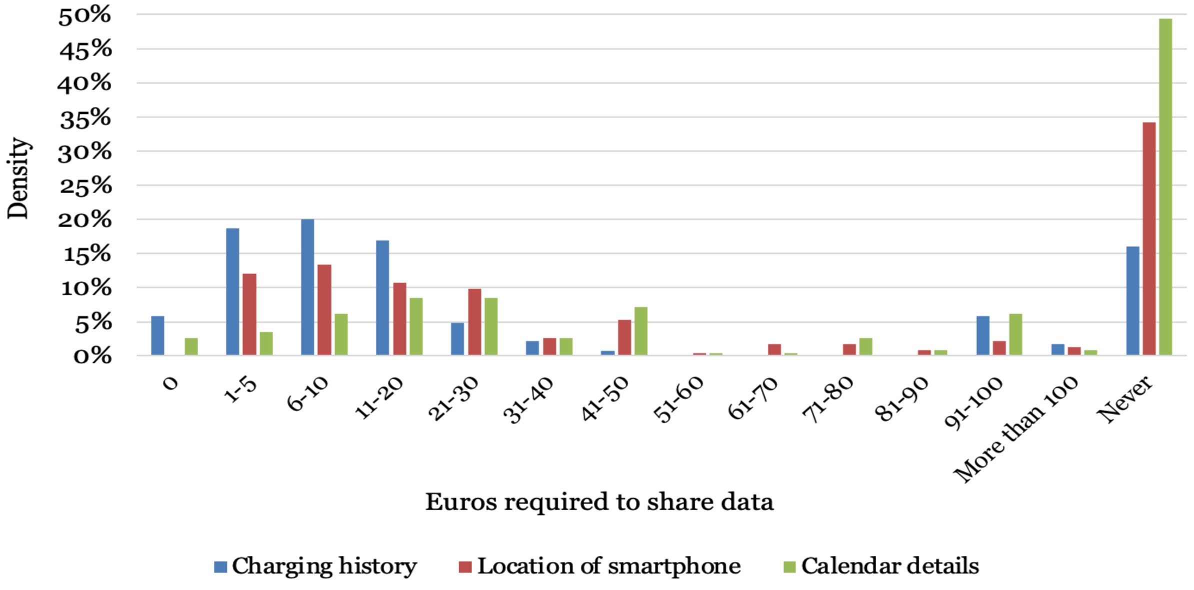

Figure 2. Euros which participants require back to share their data

We calculated the correlations between demographic variables and our main variables in an exploratory analysis. Women were less willing than men to share their calendar data (r_{Sp} = -.12, p = .012) and perceived more benefits with the smart charging application (r_{Sp} = .11, p = .017). Also, increasing age had a direct negative effect on the willingness to share location data (r = -.13, p = .005) and a direct positive effect with greater trust in their energy provider (r = .13, p = .006).

Discussion

Our findings provide food for thought about the applicability of the privacy paradox to smart charging. In our answer to RQ1 (*What data types do individuals intend to share for smart charging?),* we found that most people would share their charging history with a smart charging application. Participants are more ambivalent about their smartphone location data and are reluctant to share their calendar details. These findings are consistent with previous studies on data sharing with websites (Malhotra, 2012; Smith et al., 2011) and indicate that the readiness to share data decreases with increasing data sensitivity.

For RQ2 (*Which factors impact individual's intention to share data with their smart charging app?),* we calculated the structural equation model four times, once with the intention to share data composite score (SEM1), the intention to share charging history (SEM2), the intention to share the location of the smartphone (SEM3), and the intention to share calendar details (SEM4) as dependent variables. In general, our analysis indicates that Barth and de Jong's model is also valid in data sharing with a smart charging application. However, depending on the sensitivity of the data to be shared, not all factors, especially contextual ones, impact the intention to share data.

For all four models, trust and privacy awareness had a statistically significant negative impact on perceived risks and a positive effect on perceived benefits. That is, people who trusted their energy provider perceived fewer risks and more benefits with the smart charging application. While the role of institution-based trust is well-researched for customer loyalty (Utz et al., 2023) and e-commerce (McKnight & Choudhury, 2006), it also appears to play an important role for the readiness to share sensitive data with a service provider. Furthermore, people with greater awareness of privacy perceived greater risks. The general perception of greater risks in a data sharing context highlights the importance of information on data use and full transparency. This is in line with findings on risk-taking behavior, which show that the information available to individuals has a significant influence on their risk behavior (Turel, 2021).

For SEM1-3, perceived risks had a negative influence, and perceived benefits had a significant positive impact on the general intention to share data. These results align with the risk-benefit calculation since perceived benefits are often weighed against the risk probability. The higher the benefits, the easier it is to level perceived risks (Barth & de Jong, 2017; Culnan & Armstrong, 1999). However, for calendar data (SEM4), the perceived benefits of the smart charging application did not influence the intention to share data. They were insufficient to push the curve from high-risk low-benefit to high-risk high-benefit, which encouraged risk-averse behavior (Turel, 2021). The perceived risk of sharing sensitive data outweighed the perceived benefits of personalized charging, which has created a negative reward-utility balance and triggered risk averse behavior (Turel, 2021). These explanations from risk-sensitivity and foraging theory explicate risk-benefit calculations of Barth and de Jong's (2017) framework, wherein users refrain from sharing data when the risk probability is unfavorable. However, the underscoring of perceived benefits as opposed to the perceived risks of sharing sensitive data for smart charging can have significant implications for the design of smart charging applications. Either users enter their charging preferences for every charging event, which will be inconvenient, or smart charging will be limited. The success of smart charging depends on the ability to collect and analyze data to optimize charging processes.

Prior location-sharing habits had a statistically significant impact on the intention to share data for the composite score (SEM1), location data (SEM3), and calendar data (SEM4) but not for charging history (SEM2). This finding aligns with research on data sharing habits in the context of the privacy paradox (Awad & Krishnan, 2006). Despite privacy concerns, people overshare sensitive data on, for instance, social media (e.g., Chakraborty et al. 2013). Since experience-based trust might also be extendable to the action and not tied exclusively to the institution, people right- or wrongfully assume that sharing previously disclosed data does not carry any substantial risk (McKnight et al., 1998).

Our analysis of contextual factors demonstrated that the desired automation of the application positively influenced the intention to share data for the composite score (SEM1) and location data (SEM3) but not for historical data (SEM2) or calendar data (SEM4). This reflects findings from previous research on the privacy paradox wherein controlling the terms under which sensitive information is acquired and used was a key component of user privacy (Awad & Krishnan, 2006). While automation of data sharing would tremendously improve personalization and user experience, users appear reluctant to share such information unconditionally.

Despite the level of desired control, our analysis of RQ3 (*How much does the monetary incentive need to be for individuals to share different data types for smart charging?*) revealed that more than 50% of the participants would share all data types (historical data/pattern, location data, calendar data) in exchange for money. The more sensitive the data, the higher the expected monetary reward. For charging history data, over half of the participants required 20% of their monthly charging costs to be recovered. For the location of the smartphone, more than half of the participants wanted 40% of their monthly charging costs to be recovered. For calendar details, more than half of the participants required at least 100% of their monthly charging costs to be recovered. These findings reflect behavior explained in risk-sensitivity and foraging theory. The higher the risk, the higher the required benefits to switch from risk-averse to risk-prone behavior (Stephens & Charnov, 1982; Stephens & Krebs, 1986). However, the required monetary compensation may exceed what electricity companies would be willing to pay for the data.

Moreover, the results of RQ3 appear to contradict those of the model. Although the SEM model indicates that people would not share their data for money, more than 50% of our participants were willing to share all data types when explicitly asked how much (RQ3). However, the desired monetary compensation was exceptionally high for sensitive data, which is not always consistent with previous research. Dependending on the survey design, previous studies yielded different results: Braghin and Del Vecchio (2017), for instance, conducted a study in which only 36% of the participants agreed to share their browsing habits on an app for money. In contrast, Barak et al. (2013) conducted a field study asking participants for the amount required to share their location data. They found that 80% of the participants would share their location data for significant monetary rewards, while 20% would not share their data at all. Wagner et al. (2018) reviewed the existing literature on data monetarization and concluded that the monetary value of privacy is still unclear. They noted that the value people assign to their private information is generally low and that some people would sell data for only a little money. Also, Acquisti et al. (2013) suggest that privacy valuation depends on the situation's context and framing.

Theoretical and practical implications

Our research has both theoretical and practical implications. The theoretical implications of our study lie in the extension of Barth and de Jong's (2017) theoretical framework for smart charging applications. Since Cichy et al. (2021) argue in their study on data sharing for connected cars that common data sharing reservations in online service contexts do not apply to IoT devices, we demonstrated that the privacy paradox and typical data sharing reservations apply to smart charging applications. Depending on the type of data they share, users can decide on the level of personalization with a high level of control over their private information (Awad & Krishnan, 2006; McKnight et al., 1998).

However, the framework does not apply to highly sensitive calendar data. In this case, the perceived benefits of the smart charging app had no impact on the intention to share data. This demonstrates the influence of behavioral principles from foraging theory and risk-sensitivity on the data sharing intention. More specifically, some data carry inherent high-risk characteristics, which cannot be balanced even by high perceived rewards from a usability and knowledge perspective (Stephens & Charnov, 1982; Stephens & Krebs, 1986). However, findings on the effects of monetary rewards indicate differences in the value of rewards. That is, experience-based values, such as usability or convenience, appear less influential than material values in the form of concrete monetary rewards. Thus, adding of foraging and risk-sensitivity theory principles to the framework enhances Barth and de Jong's (2017) explainability of discrepancies between perceived risks and benefits.

Our findings on the effect of monetary rewards also highlight the importance of the research design to reliably catch such tendencies despite self-reporting bias. While undefined monetary rewards did not affect the readiness to share data, a direct question on the amount of money for which participants would share their data yielded different results. More than 50% of the participants were willing to share all data types. Thus, researchers might require more direct questions in their studies on the privacy paradox to reliably capture the impact of monetary incentives on data sharing.

Regarding practical implications, we found that customers are willing to share their data if they receive monetary compensation. However, the requested amount is often unrealistically high, especially for sensitive data such as calendar and smartphone, and may not be financially attractive to energy providers.

In addition, we found that perceived risks and benefits of the smart charging app have a significant impact on people's willingness to share data. Energy providers should, therefore, ensure that customers are well-informed about the benefits of their application and the use of data for smart charging to lower perceived risks. Explanatory videos might help convey the required information.

Furthermore, it is a good idea for energy providers to limit data collection to only the essential information needed to further optimize the charging process. This approach will help to avoid the unnecessary collection of data that may concern users.

Trust in the energy provider also influences how participants perceive the risks and benefits of the application. It is therefore important for energy providers to build trust with their customers. This can be done by being transparent about how they collect, process, and use data, or through, for instance, customer loyalty programs based on transparency-enhancing technology (e.g. Utz et al. 2023).

Limitations and future work

Our research comes with some limitations. First, we measured the intention to share data but not the actual behavior. There may be a gap between intention and actual behavior (Sheeran & Webb, 2016). A field study measuring the actual behavior could help us fill the gap but would have to be postponed until smart charging is more widely adopted. This is also the reason why we restricted our study to the intention of sharing data.

Second, we applied the rational decision-making framework to smart charging, which assumes that data sharing is rational. However, our decisions are also influenced by biases such as heuristics and situational cues (Barth & de Jong, 2017). To meet this limitation, future research could carry out a pilot focusing on irrational factors influencing decision-making.

Third, we asked participants for the amount of money rewards required to share their data. However, this self-assessment may not necessarily correspond to the actual values at which they would share their data. To overcome this limitation, a randomized experimental study could be conducted to test for how much money participants would be willing to share their data.

Fourth, we need to consider the possibility that our findings may not generalize to other cultural groups. Researchers claim that people from individualistic cultures value privacy more and show more privacy-protective behaviors, while in collectivistic cultures, privacy is less protected (Li, 2022). A cross-cultural study would help us evaluate the generalizability of our findings. However, previous cross-cultural studies on social networks often did not show differences between individualist and collectivist cultures (Li, 2022).

Conclusion

Our research aimed to investigate the types of data individuals would share with a smart charging application for EVs, such as charging patterns, smartphone location, and calendar details, and the factors influencing their decision. We applied the theoretical framework of Barth and de Jong (2017) and conducted a large-scale online survey to explore our hypotheses. We also investigated if participants would share their data for monetary rewards and, dependent on the data type, for how much. We used the IS theories of the privacy paradox (e.g., Barth and de Jong, 2017), foraging theory, and risk sensitivity theory to explore this behavior (e.g., Turel 2021)

We found that most individuals would share their charging history but would not share more sensitive data, such as calendar details. Participants were also ambivalent about sharing the location data. To determine which factors influenced the decision to share data, we calculated four SEM models, each with one dependent variable – charging details, smartphone location, calendar data – and a composite score of all three variables. The perceived risks and benefits of the smart charging application determined the intention to share charging details and smartphone location. However, perceived benefits did not influence the decision to share sensitive calendar data, while perceived risks had a significant influence.

Moreover, we discovered that different contextual factors influenced the data sharing decision for different data types. For instance, the desired degree of automation, influenced the intention to share location data but not the intention to share the charging history and calendar data. Interestingly, proposed monetary rewards did not have a significant impact on the intention to share data in any of the SEM models. However, when we asked participants from the monetary rewards group how much money they would share their data, most participants indicated willingness to share data for a monetary reward. The requested amount increased with the sensitivity of the data. Therefore, the energy supplier needs to decide if it is worth paying these rewards to get access to relevant data for smart charging.

Acknowledgements

This research was funded in part by the Luxembourg National Research Fund (FNR) and PayPal, PEARL grant reference 13342933/Gilbert Fridgen. For the purpose of open access, the authors have applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any Author Accepted Manuscript version arising from this submission. Additionally, the authors gratefully acknowledge the Fondation Enovos under the aegis of the Fondation de Luxembourg in the frame of the philanthropic funding for the research project INDUCTIVE which is the initiator of this applied research. We thank Dr. Valerie Graf-Drasch, Dr. Mohammad Ansarin, and Dr. Michael Schöpf for their input regarding the study design.

References

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What Is privacy worth? *The Journal of Legal Studies*, *42*(2), 249–274. **https://doi.org/10.1086/671754**

Ajzen, I. (1985). *From intentions to actions: A theory of planned behavior*. Springer.

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predictiing social behavior*. Prentice-Hall.

Aloise-Young, P. A., Lurbe, S., Isley, S., Kadavil, R., Suryanarayanan, S., & Christensen, D. (2021). Dirty dishes or dirty laundry? Comparing two methods for quantifying American consumers' preferences for load management in a smart home. *Energy Research & Social Science*, *71*, 101781. **https://doi.org/10.1016/j.erss.2020.101781**

Alotaibi, A. K., Barros, A. P., & Degirmenci, K. (2023). Co-Creating Value from Electric Vehicle Digital Services: Effect of Perceived Environmental Performance on Personal Data Sharing. *European Conference on Information Systems*.

Awad & Krishnan. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. *MIS Quarterly*, *30*(1), 13. **https://doi.org/10.2307/25148715**

Bailey, J., & Axsen, J. (2015). Anticipating PEV buyers' acceptance of utility controlled charging. *Transportation Research Part A: Policy and Practice*, *82*, 29–46. **https://doi.org/10.1016/j.tra.2015.09.004**

Barak, O., Cohen, G., Gazit, A., & Toch, E. (2013). The price is right?: Economic value of location sharing. *Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication*, 891–900. **https://doi.org/10.1145/2494091.2497343**

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. **https://doi.org/10.1016/j.tele.2017.04.013**

Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, *41*, 55–69. **https://doi.org/10.1016/j.tele.2019.03.003**

Bhusal, N., Gautam, M., & Benidris, M. (2021). Cybersecurity of Electric Vehicle Smart Charging Management Systems. *2020 52nd North American Power Symposium (NAPS)*, 1–6. **https://doi.org/10.1109/NAPS50074.2021.9449758**

Braghin, C., & Del Vecchio, M. (2017). Is Pokémon GO watching you? A survey on the privacy-awareness of location-based apps' users. *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, 164–169. **https://doi.org/10.1109/COMPSAC.2017.158**

Brey, B. de, Gardien, L., & Hiep, E. (2021). Smart charging needs, wants and demands, charging experiences and opinions of EV drivers. *World Electric Vehicle Journal*, *12*(4), 168. **https://doi.org/10.3390/wevj12040168**

Brey, J. J., Brey, R., Contreras, I., & Carazo, A. F. (2014). Roll-out of hydrogen fueling stations in Spain through a procedure based on data envelopment analysis. *International Journal of Hydrogen Energy*, *39*(8), 4116–4122. **https://doi.org/10.1016/j.ijhydene.2013.09.141**

Caraco, T., Martindale, S., & Whittam, T. S. (1980). An empirical demonstration of risk-sensitive foraging preferences. *Animal Behaviour*, *28*(3), 820–830. **https://doi.org/10.1016/S0003-3472(80)80142-4**

Cartar, R. V. (1991). A Test of Risk-Sensitive Foraging in Wild Bumble Bees. *Ecology*, *72*(3), 888–895. **https://doi.org/10.2307/1940590**

Chakraborty, R., Vishik, C., & Rao, H. R. (2013). Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. *Decision Support Systems*, *55*(4), 948–956. **https://doi.org/10.1016/j.dss.2013.01.004**

Cichy, P., Salge, T. O., & Kohli, R. (2021). Privacy concerns and data sharing in the internet of things: Mixed methods evidence from connected cars. *MIS Quarterly*, *45*(4), 1863-1892. **https://doi.org/10.25300/MISQ/2021/14165**

Cohen, J. (2013). *Statistical power analysis for the behavioral sciences*. Routledge.

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**

Daina, N., Sivakumar, A., & Polak, J. W. (2017). Modelling electric vehicles use: A survey on the methods. *Renewable and Sustainable Energy Reviews*, *68*, 447–460. **https://doi.org/10.1016/j.rser.2016.10.005**

Develder, C., Sadeghianpourhamami, N., Strobbe, M., & Refa, N. (2016). Quantifying flexibility in EV charging as DR potential: Analysis of two real-world data sets. *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 600–605. **https://doi.org/10.1109/SmartGridComm.2016.7778827**

Döbelt, S., Jung, M., Busch, M., & Tscheligi, M. (2015). Consumers' privacy concerns and implications for a privacy preserving Smart Grid architecture—Results of an Austrian study. *Energy Research & Social Science*, *9*, 137–145. **https://doi.org/10.1016/j.erss.2015.08.022**

Donnenwerth, G. V., & Foa, U. G. (1974). Effect of resource class on retaliation to injustice in interpersonal exchange. *Journal of Personality and Social Psychology*, *29*(6), 785–793. **https://doi.org/10.1037/h0036201**

Eldeeb, H. H., Faddel, S., & Mohammed, O. A. (2018). Multi-objective optimization technique for the operation of grid tied PV powered EV charging station. *Electric Power Systems Research*, *164*, 201–211. **https://doi.org/10.1016/j.epsr.2018.08.004**

Fernández, J. D., Menci, S. P., Lee, C. M., Rieger, A., & Fridgen, G. (2022). Privacy-preserving federated learning for residential short-term load forecasting. *Applied Energy*, *326*, 119915. **https://doi.org/10.1016/j.apenergy.2022.119915**

Foa, U. G. (1971). Interpersonal and economic resources: Their structure and differential properties offer new insight into problems of modern society. *Science*, *171*(3969), 345–351. **https://doi.org/10.1126/science.171.3969.345**

Fortes, N., Rita, P., & Pagani, M. (2017). The effects of privacy concerns, perceived risk and trust on online purchasing behaviour. *International Journal of Internet Marketing and Advertising*, *11*(4), 307. **https://doi.org/10.1504/IJIMA.2017.087269**

Fox, G. (2020). To protect my health or to protect my health privacy? A mixed-methods investigation of the privacy paradox. *Journal of the Association for Information Science and Technology*, *71*(9), 1015–1029. **https://doi.org/10.1002/asi.24369**

Fridgen, G., Mette, P., & Thimmel, M. (2014). The Value of Information Exchange in Electric Vehicle Charging. *ICIS 2014 Proceedings*. **https://aisel.aisnet.org/icis2014/proceedings/ConferenceTheme/4**

Guthoff, F., Klempp, N., & Hufendiek, K. (2021). Quantification of the Flexibility Potential through Smart Charging of Battery Electric Vehicles and the Effects on the Future Electricity Supply System in Germany. *Energies*, *14*(9), 2383. **https://doi.org/10.3390/en14092383**

Habbak, H., Baza, M., Mahmoud, M. M. E. A., Metwally, K., Mattar, A., & Salama, G. I. (2022). Privacy-Preserving Charging Coordination Scheme for Smart Power Grids Using a Blockchain. *Energies*, *15*(23), Article 23. **https://doi.org/10.3390/en15238996**

Hair, J. F. (Ed.). (2017). *A primer on partial least squares structural equations modeling (PLS-SEM)*. SAGE.

Hirschprung, R., Toch, E., Bolton, F., & Maimon, O. (2016). A methodology for estimating the value of privacy in information disclosure systems. *Computers in Human Behavior*, *61*, 443–453. **https://doi.org/10.1016/j.chb.2016.03.033**

IEA. (2022). *Global EV Outlook 2022 Securing supplies for an electric future* (pp. 1–221).

IRENA. (2019). *Innovation Landscape brief: Electric-vehicle smart charging*. International Renewable Energy Agency (IRENA). **https://books.google.lu/books?id=Kh0DEAAAQBAJ**

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, *44*(2), 544–564. **https://doi.org/10.1016/j.dss.2007.07.001**

Kim, D., Park, K., Park, Y., & Ahn, J.-H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, *92*, 273–281. **https://doi.org/10.1016/j.chb.2018.11.022**

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. **https://doi.org/10.1016/j.cose.2015.07.002**

Kolotylo-Kulkarni, M., Xia, W., & Dhillon, G. (2021). Information disclosure in e-commerce: A systematic review and agenda for future research. *Journal of Business Research*, *126*, 221–238. **https://doi.org/10.1016/j.jbusres.2020.12.006**

Kramer, J., & Petzoldt, T. (2022). A matter of behavioral cost: Contextual factors and behavioral interventions interactively influence pro-environmental charging decisions. *Journal of Environmental Psychology*, *84*, 1–9. **https://doi.org/10.1016/j.jenvp.2022.101878**

Li, Y. (2022). Cross-cultural privacy differences. In *Modern Socio-Technical Perspectives on Privacy* (pp. 267–292). Springer International Publishing Cham.

Malhotra, P. (2012). Recruitment and Training of Higher Civil Service: A Case for Change. *Indian Journal of Public Administration*, *58*(3), 544–551. **https://doi.org/10.1177/0019556120120323**

McKnight, D. H., & Choudhury, V. (2006). Distrust and trust in B2C e-commerce: Do they differ? *Proceedings of the 8th International Conference on Electronic Commerce The New E-Commerce: Innovations for Conquering Current Barriers, Obstacles and Limitations to Conducting Successful Business on the Internet - ICEC '06*, 482. **https://doi.org/10.1145/1151454.1151527**

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial Trust Formation in New Organizational Relationships. *The Academy of Management Review*, *23*(3), 473. **https://doi.org/10.2307/259290**

McMahan, B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. y. (2017). Communication-Efficient Learning of Deep Networks from Decentralized Data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, 1273–1282. **https://proceedings.mlr.press/v54/mcmahan17a.html**

Mishra, S., & Fiddick, L. (2012). Beyond gains and losses: The effect of need on risky choice in framed decisions. *Journal of Personality and Social Psychology*, *102*(6), 1136–1147. **https://doi.org/10.1037/a0027855**

Ouellette, J. A., & Wood, W. (1998). Habit and intention in everyday life: The multiple processes by which past behavior predicts future behavior. *Psychological Bulletin*, *124*(1), 54–74. **https://doi.org/10.1037/0033-2909.124.1.54**

Papaefthymiou, G., Haesen, E., & Sach, T. (2018). Power System Flexibility Tracker: Indicators to track flexibility progress towards high-RES systems. *Renewable Energy*, *127*, 1026–1035. **https://doi.org/10.1016/j.renene.2018.04.094**

Pawlowski, T., & Dinther, C. van. (2020). Assessing the Impact of Electric Vehicle Charging Behavior on the Distribution Grid. *AMCIS 2020 Proceedings*. **https://aisel.aisnet.org/amcis2020/sig_green/sig_green/12**

Payne, B. K., Brown-Iannuzzi, J. L., & Hannay, J. W. (2017). Economic inequality increases risk taking. *Proceedings of the National Academy of Sciences*, *114*(18), 4643–4648. **https://doi.org/10.1073/pnas.1616453114**

Ponnurangam Kumaraguru, & Cranor, L. Faith. (2005). *Privacy indexes: A survey of Westin's studies*. 1341067 Bytes. **https://doi.org/10.1184/R1/6625406.V1**

Rosseel, Y. (2012). Lavaan: An R package for structural equation modeling. *Journal of Statistical Software*, *48*(2). **https://doi.org/10.18637/jss.v048.i02**

Saxena, S., MacDonald, J., Black, D., & Kiliccote, S. (2015). *Quantifying the Flexibility for Electric Vehicles to Offer Demand Response to Reduce Grid Impacts without Compromising Individual Driver Mobility Needs*. 2015-01–0304. **https://doi.org/10.4271/2015-01-0304**

Schmidt, J., & Busse, S. (2013). The Value of IS to Ensure the Security of Energy Supply – The Case of Electric Vehicle Charging. *AMCIS 2013 Proceedings*. **https://aisel.aisnet.org/amcis2013/GreenIS/GeneralPresentations/6**

Shah, R. (2015). *Do Privacy Concerns Really Change With The Internet of Things?* Forbes.

Sheeran, P., & Webb, T. L. (2016). The Intention-Behavior Gap: The Intention-Behavior Gap. *Social and Personality Psychology Compass*, *10*(9), 503–518. **https://doi.org/10.1111/spc3.12265**

Shepardson, D., Klayman, B., & Klayman, B. (2021, December 8). U.S. government to end gas-powered vehicle purchases by 2035 under Biden order. *Reuters*. **https://www.reuters.com/world/us/biden-pledges-end-gas-powered-federal-vehicle-purchases-by-2035-2021-12-08/**

Smith, H. J. (2008). Information privacy and its management. *MIS Quarterly Executive*, *3*(4), 6. **https://aisel.aisnet.org/misqe/vol3/iss4/6**

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1015. **https://doi.org/10.2307/41409970**

Söllner, M., Hoffmann, A., & Leimeister, J. M. (2016). Why different trust relationships matter for information systems users. *European Journal of Information Systems*, *25*(3), 274–287. **https://doi.org/10.1057/ejis.2015.17**

Söllner, M., Mishra, A. N., Becker, J.-M., & Leimeister, J. M. (2022). Use IT again? Dynamic roles of habit, intention and their interaction on continued system use by individuals in utilitarian, volitional contexts. *European Journal of Information Systems*, 1–17. **https://doi.org/10.1080/0960085X.2022.2115949**

Soper, D. S. (2022). *A-priori sample size calculator for structural equation models [Software]* [Computer software]. **https://www.danielsoper.com/statcalc**

Stephens, D. V., & Charnov, E. L. (1982). *Optimal foraging: Some simple stochastic models*. Behavioral Ecology and Sociobiology.

Stephens, D. V., & Krebs, J. R. (1986). *Foraging theory* (Vol. 6). Princeton university press.

Strüker, J., & Kerschbaum, F. (2012). From a Barrier to a Bridge: Data-Privacy in Deregulated Smart Grids. *ICIS 2012 Proceedings*. **https://aisel.aisnet.org/icis2012/proceedings/BreakthroughIdeas/2**

Teng, F., Chhachhi, S., Ge, P., Graham, J., & Gunduz, D. (2022). *Balancing privacy and access to smart meter data: An Energy Futures Lab briefing paper*. Imperial College London. **https://doi.org/10.25561/96974**

Turel, O. (2021). Technology-Mediated Dangerous Behaviors as Foraging for Social-Hedonic Rewards: The Role of Implied Inequality. *MIS Quarterly*, *45*(3), 1249–1286. **https://doi.org/10.25300/MISQ/2021/16353**

Utz, M., Johanning, S., Roth, T., Bruckner, T., & Strüker, J. (2023). From ambivalence to trust: Using blockchain in customer loyalty programs. *International Journal of Information Management*, *68*, 102496. **https://doi.org/10.1016/j.ijinfomgt.2022.102496**

van der Meer, D., Chandra Mouli, G. R., Morales-Espana Mouli, G., Elizondo, L. R., & Bauer, P. (2018). Energy Management System With PV Power Forecast to Optimally Charge EVs at the Workplace. *IEEE Transactions on Industrial Informatics*, *14*(1), 311–320. **https://doi.org/10.1109/TII.2016.2634624**

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, *7*(6), 1. **https://aisel.aisnet.org/jais/vol7/iss6/16**

Wagner, A., Wessels, N., Buxmann, P., & Krasnova, H. (2018). Putting a price tag on personal information-A literature review. *Proceedings of the 51st Hawaii International Conference on System Sciences*, 1–10.

Westland, J. C. (2010). Lower bounds on sample size in structural equation modeling. *Electronic Commerce Research and Applications*, *9*(6), 476–487. **https://doi.org/10.1016/j.elerap.2010.07.003**

Wong, S. D., Shaheen, S. A., Martin, E., & Uyeki, R. (2023). Do incentives make a difference? Understanding smart charging program adoption for electric vehicles. *Transportation Research Part C: Emerging Technologies*, *151*, 104123. **https://doi.org/10.1016/j.trc.2023.104123**

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. *ICIS 2012 Proceedings*, 1–16.

Xu, H., Rosson, M. B., & Carroll, J. M. (2008). Mobile user's privacy decision making: Integrating economic exchange and social justice perspectives. *AMCIS 2008 Proceedings*, 1–10. **https://aisel.aisnet.org/amcis2008/179**