Groping in the dark? Exploring customer perception of hidden actions in smart service ecosystems through the lens of agency theory

Ronja Schwinghammer
LMU Munich School of
Management
schwinghammer@lmu.de

Abstract

Due to new technologies, providers of digital goods and services collect an ever-increasing amount of personal data. Although the GDPR mandates that providers must inform their customers about the handling of their data, past privacy scandals have shown that customers lack information. In this study, we adopt a qualitative-exploratory approach to develop a rich understanding of the practices about which customers are not fully informed. We rely on agency theory to understand hidden actions as an informational advantage of providers. By conducting focus groups, we identify perceptions of three key hidden actions of smart product customers in B2C service ecosystems. Building on the hidden actions, we understand the relationship between customer and provider in smart service ecosystems characterized by information asymmetries. With our research, we provide the first steps towards understanding the nature and role of hidden actions in the context of smart service ecosystems. For practitioners, we provide guidance on how to effectively reduce information asymmetries.

Keywords: Personal data, smart product, smart service ecosystem, hidden action, agency theory.

1. Introduction

New technologies like the Internet of Things (IoT) empower digital service providers to amass increasing personal data (Lim et al., 2018; Cichy et al., 2021). Data-based business models further enable versatile data usage, from personalized offers to data sales (Parvinen et al., 2020). Privacy advocates, however, emphasize the hidden, privacy-invasive practices that often escape customers' awareness. For instance, Fitbit allows Google to use health data for targeted ads unbeknownst to customers (Bourreau et al., 2020). Regulatory efforts like the General Data Protection Regulation (GDPR) enforce data handling via "notice and consent" (GDPR, 2016). However, past breaches, like Cambridge Analytica, reveal that customers are often poorly informed about providers' practices (Frier, 2018). This gap arises from complex privacy measures, but also from opportunistic behavior of providers or the expanded scope of data processing (Acquisti et al., 2020).

Data-based business models create novel information asymmetries (Trzaskowski, 2022). Major platform providers like Google, Facebook, or Netflix often possess more customer insights, allowing them to influence purchasing decisions and information consumption via filter bubbles (Trzaskowski, 2022). This information asymmetry is exacerbated when providers collect more data than disclosed or use it for unexpected purposes (Al-Natour et al., 2020). Prior IS research shows that data collection and analysis is becoming more sophisticated and privacy risks are increasing (Liu et al., 2022; Gerlach et al., 2015). However, customers struggle to assess risks of data disclosure due to opaque data handling (Chang & Chen, 2014; Al-Natour et al., 2020). Prior IS studies draw on agency theory to illustrate providers' ability to mask their actions (e.g., Pavlou et al., 2007; Al-Natour et al., 2020). Hidden actions can be understood as a type of information asymmetry that occurs after the purchase of a digital good or service (Eisenhardt, 1989; Al-Natour et al., 2020). However, existing privacy measures, such as policies or "notice and consent," often inadequately mitigate information asymmetries (Tsai et al., 2011; Trzaskowski, 2022; Acquisti et al., 2020).

In the absence of practice-related information, customers cannot weigh the risks against the benefits of disclosing data (Smith et al., 2011). Consequently, privacy decisions are increasingly made amidst uncertainty (e.g., Al-Natour et al., 2020; Liu et al., 2022; Acquisti et al., 2018; Trzaskowski, 2022). Notably, the extent of practices by smart product providers remains uncertain for their customers (Cichy et al., 2021). However, the specific practices about which customers lack information remain unclear. Against this backdrop, we build on the theoretical

URI: https://hdl.handle.net/10125/106898
978-0-9981331-7-1

concept of hidden actions (Eisenhardt, 1989) to address the research question: *What actions of providers are perceived as hidden by smart product customers in B2C service ecosystems?*

To answer our research question, we adopt a qualitative-exploratory research approach and conduct focus groups. Our contribution lies in identifying three key hidden actions perceived by customers of smart products. Further, we synthesize IS research strands on privacy uncertainty and ecosystems by delving into the role of hidden actions in B2C service ecosystems. Below, we provide an overview of the pertinent literature and agency theory. Next, we delineate our methodology and explain the identified hidden actions. We discuss our results through the lens of agency theory to enhance understanding of the construct of hidden actions in smart service ecosystems. Finally, we present implications, limitations, and further research.

2. Related literature and theoretical background

2.1. Smart products and service ecosystems

IoT and smart products are rapidly integrating into our daily lives through applications in various domains, including households, healthcare and fitness, and transportation (Cichy et al., 2021; Lim et al., 2018). Smart products, equipped with sensors and connectivity, gather data from their surroundings and sometimes interact with them (Porter & Heppelmann, 2014). This combination of IoT technology and diverse applications enables smart products to capture novel customer-related data, such as energy consumption data from smart meters or driving statistics from smart vehicles (Warkentin et al., 2017; Lim et al., 2018). Smart products offer value beyond their physical attributes, serving as a foundation for delivering smart services (Beverungen et al., 2019; Herterich et al., 2023). In the B2C context, smart products are often bundled with smartphone applications that enable customers to access and interpret their data, ranging from fitness metrics to driving behavior (Lim et al., 2018).

Service ecosystems form around smart products to leverage the data they collect (Adner, 2017; Beverungen et al., 2019; Herterich et al., 2023). In the realm of smart services, value is not unilaterally generated by a single actor (Lusch & Nambisan, 2015; Lim & Maglio, 2018; Herterich et al., 2023; Beverungen et al., 2019). Rather, it is a collaborative effort involving various actors, technologies, and data to achieve mutual benefits (Lim & Maglio, 2018; Herterich et al., 2023). Customers play a vital role in co-creating value by sharing their data through smart products and receiving valuable information in return (Vargo, 2008; Lim et al., 2018). Smart services can offer functional, hedonic, or social value to customers (Paukstadt et al., 2019). Meanwhile, smart product providers primarily capture value in monetary terms (Knote et al., 2022), such as by selling data for targeted advertising or complementary services (Beverungen et al., 2019; Porter & Heppelmann, 2014).

2.2. Agency theory in IS

Agency theory posits that principals instruct agents to act on their behalf (Eisenhardt, 1989). The principal delegates a task or responsibility but cannot control the actions of the agent. Conflicts can arise due to differing objectives and interests (Eisenhardt, 1989). In online market buyers (principals) delegate the responsibility of product delivery to sellers (agents) as depicted in Figure 1. However, buyers face uncertainty in assessing product quality (Pavlou et al., 2007). Sellers strive for profit, while buyers focus on assured quality and delivery. As the agent's actions may not be fully transparent, ensuring alignment with the principal's interests become challenging.

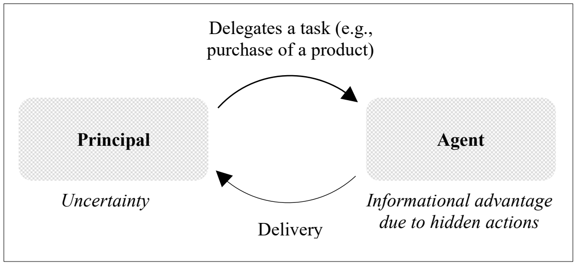
Delegates a task (e.g., purchase of a product)
Principal
Agent
Uncertainty
Delivery
Informational advantage due to hidden actions

Figure 1. Principal-agent situation in online marketplaces.

In agency theory, hidden actions encompass agent behaviors unobservable to the principal (Eisenhardt, 1989). This form of information asymmetry can increase uncertainty and potential problems in aligning interests (Mishra et al., 1998). In e-commerce, sellers' hidden actions could manifest as subpar product quality or delayed delivery (Pavlou et al., 2007). However, as digital goods and services surge, hidden actions increasingly relate to the handling of personal data (Al-Natour et al., 2020; Chang & Chen, 2014). Even post-purchase, providers collect data, often with unclear intent to their customers (Al-Natour et al., 2020). For instance, mobile apps leverage location or usage data for targeted ads. Hidden actions make customers unaware of privacy risks, which reduces their willingness to use a service (Al-Natour et al., 2020).

In principal-agent scenarios, agents use signals to alleviate uncertainty and assure principals that their behavior lacks opportunism (Eisenhardt, 1989). For instance, online marketplaces employ informational signals, such as pre-purchase privacy policies and post-purchase trust signals (Pavlou et al., 2007). However, prior research shows that privacy policies or "notice and consent" often fail to adequately inform customers (Tsai et al., 2011; Trzaskowski, 2022). Thus, customers often lack comprehensive insights into data practices, necessitating reliance on providers for trustworthy data handling (Acquisti et al., 2020; Al-Natour et al., 2020).

Prior IS studies have relied on agency theory to illustrate how customers of digital products or services make privacy decisions amid uncertainty (e.g., Al-Natour et al., 2020). Building upon this foundation, we show that assumptions of agency theory regarding informational advantage, hidden action, opportunistic behavior, and signaling are applicable to buyer-seller relationships (e.g., Pavlou et al., 2007). To address our research objective, we employ the theoretical concept of hidden action to investigate the practices of smart product providers about which customers are not fully informed (Eisenhardt, 1989). In doing so, we rely on the assumption that providers have an interest in not fully disclosing their actions (Eisenhardt, 1989).

3. Methodology

3.1. Qualitative-empirical approach

We adopt a qualitative-exploratory approach to investigate individuals' perceptions of hidden actions. Customers often feel inadequately informed and insecure regarding data collection and use before and after purchasing digital goods or services (Pavlou et al., 2007; Al-Natour et al., 2020). Providers motivated by incentives to maintain information asymmetry may compromise customer privacy or increase uncertainty. Lengthy and complex privacy measures, such as policies, are often unable to reduce information asymmetry because they cognitively overwhelm customers (Acquisti et al., 2020). Additionally, providers may employ strategies resembling dark patterns to nudge data disclosure (Gawer, 2022). While prior IS studies empirically confirm that asymmetric information from hidden actions leads to uncertainty, a comprehensive understanding of hidden actions is lacking (e.g., Al-Natour et al., 2020). Hence, our primary research goal is to comprehend hidden actions from a customer-centric perspective. Through an exploration of their thoughts, narratives, and perceptions, we aim to unveil actions that customers may lack information despite existing privacy measures (Eisenhardt, 1989). Due to the limited awareness of smart product customers regarding providers' practices (Cichy et al., 2021), we conducted focus group interviews with B2C smart product users, as detailed below.

3.2. Data collection and analysis

We conducted ten focus groups comprising 37 participants who use smart products across various applications, including household, health, fitness, and mobility (Cichy et al., 2021). These applications involve diverse devices, such as smartwatches, smart speakers, smart meters, lighting, and cars. Each focus group consisted of three to four participants, with sessions lasting 50 to 70 minutes. To ensure diverse perspectives, we recruited participants across various demographic characteristics, including gender, age, education, and profession (see Table 1). We obtained this sample through a combination of opportunistic sampling and peer recruitment.

Focus groups are most fruitful when participants engage in discussions that allow for "structured eavesdropping" (Kitzinger, 1995, p. 301). Hence, we formed groups with homogeneous demographics, as this often encourages peers to express their genuine opinions more comfortably (Karwatzki et al., 2017). We followed Fern's (2001) guidelines regarding the duration, moderation, and design of our semi-structured interview guide. At the session outset, we introduced the research context and objectives to align the groups. The interview guide covered data collection, use, and protection while allowing flexibility to adapt to the dynamics of each group. Focus groups were conducted via Zoom to include participants from Germany, Austria, and Switzerland.

Table 1. Demographics of participants.

Demographics		Frequency (Percentage)
Age	<24	12 (32.4%)
	25-29	14 (37.8%)
	>30	11 (29.7%)
Gender	Female	17 (45.9%)
	Male	20 (54.1%)
Education Level	High/Secondary	8 (21.6%)
	Bachelor	12 (32.4%)
	Master	11 (29.7%)
	PhD	6 (16.2%)
Employment Status	Employed	18 (48.6%)
	Self-employed	7 (18.9%)
	Student	12 (32.4%)
Profession	Economic	10 (27.0%)
	Technical	9 (24.3%)
	Social/Education	9 (24.3%)
	Medical/Natural science	5 (13.5%)
	Art/Service/Others	4 (10.8%)

After data collection, we transcribed and analyzed the focus group discussions. Adhering to a qualitative-exploratory approach, we commenced our analysis with iterative coding using Atlasi.ti (Corbin & Strauss, 2008). We compared participants' ideas, opinions, and thoughts, marking statements indicating a lack of information regarding provider actions following an inductive coding (Gioia, 2013). In the absence of a mature theoretical understanding of hidden actions, an inductive coding is deemed appropriate. This approach allowed for an in-depth examination of hidden actions within the complex landscape of service ecosystems. In specific, it allowed us to uncover nuanced aspects, such as the timing of data collection, that are not apparent through device usage or privacy policies alone. We could also identify categories that go beyond regulations to include data valuation or opportunistic behaviors such as non-compliance. Thus, inductive coding has enriched our findings by overcoming the limitations associated with privacy statements that represent cognitive overload or lack in-depth information. After the initial coding, we grouped codes with similar meanings to derive a total of 17 subcategories from our transcripts. In the subsequent step, we adopted axial coding (Saldaña, 2021). We established seven categories, which we distilled into three distinct perceived hidden actions. Throughout the coding process, we engaged in iterative cycles to critically assess codes with shared themes, determining whether to consolidate them.

4. Results

All participants have a general awareness of data collection and usage through their experiences with smart products and services. They mention using apps, often connected to devices such as smartwatches or smart meters, to gain insights into their data. However, despite a general understanding of data collection and use across all demographic profiles, participants are often unsure when it comes to specific measures and hesitant when it comes to, for example, the data collected, its timing, purpose, or value. They believe that providers intentionally maintain this uncertainty by inadequately disclosing their actions or by providing imprecise information when required by the GDPR. Nevertheless, through personal experiences and focus group discussions, participants have developed reasonably accurate ideas about actions for which they lack sufficient information. In total, we identified three primary perceived hidden actions, elaborated below, and organized by categories and subcategories as shown in Table 2.

Table 2. Categories and subcategories of perceived hidden actions.

Perception of hidden action	Category	Subcategory	Exemplary description
Data processing	Data collection	Data type	• What kind of data is collected? What habitual data is collected? What does the provider know about the customer? Does he know more than the customer?
		Data source	• Which data acquisition components does the provider equip the smart products with? What can the sensors, microphones, or cameras of smart products capture?
		Data scope	• Does the smart product record continuously? Are there intervals when the provider does not record?
		Data control	• Does the provider no longer record when the customer deactivates recording? Is a restriction possible for reasons of a technical functionality of the smart product?
	Data analysis	Algorithms	• How can algorithms improve the technical functionality of smart products? What are the algorithms that underlie smart products? What are their conclusions?
		Visualization	• Which visualizations are made available to the user? Does the provider withhold visualizations?
Data transmission	Device-to-device transfer	API setup	• What interfaces does the provider set up between the devices? Does the provider set up interfaces to the other personal devices (e.g., smartphone) and what can he access?
	Cloud transfer	Cloud storage	• Is the data stored in a public cloud or locally on the smart product? What is stored? For how long?
		Deletion	• What are the options for deleting data in a cloud? How can the user check whether the provider has deleted personal data? Is there a backup or residual copies?
	Third-party transfer	Regulatory compliance	• Is the provider legally authorized to share data? Does the provider always comply with current data protection? What data is transferred in countries without GDPR?
		Notice and consent	• Does the provider inform about the disclosure and by what means? Does the provider ask for consent? What purposes does the provider refer to in the consent?
		Actors	• To which organizations does the provider share the data? What are the access rights (e.g., access of de-anonymized data)? What are the purposes of data sharing?
Data monetization	Service provision	Value exchange	• What added value does the provider offer the user in return for his data? Does the user get enough in return for his data? Does the provider offer a fair exchange?
		Data value	• What monetary value does the provider place on personal data? What do others pay the provider for access to the data?
		Data aggregation	• For what purposes does the provider aggregate the data? Is there indirect or direct monetization behind it?
	Targeting	Targeted advertising	• When are personalized ads served? Based on which recorded routines and preferences? On which platforms are they played out?
		Targeted services	• What targeted services does the provider create? What are possible negative consequences? How does the provider network with relevant stakeholder?

4.1. Processing of data

The focus groups describe a perception of hidden actions by the provider related to the processing of their personal data. Data processing captures the categories collection and analysis of personal data. First, for data collection, the subcategories are data type, source, scope, and control.

Data type reflects the lack of information about what type of data smart product providers collect. Although all focus group participants are aware to some extent of the collection of their data, they are often unaware of the many types of data. In immediate response to the question of what kind of data might be collected, one participant replied, “Now I’m in the dark” (I2). However, participants believe that “data is recorded that they do not know about” (I2). Upon reflection, customers believe that providers might collect their location data, audio data, or routines and preferences: “(...) when I think of Alexa, then of course all habits can be recorded. So, when do you get up, when do you go to bed, for example, with the light. What music do you listen to?” (I5). With the many types of collected data, participants often wonder, ‘what does the provider know about me?’

Data source captures the lack of information about what components of the smart product collect data. The participants do not know what data the providers collect with sensors, microphones, or cameras: “(…) at the beginning I was worried because my smart robot vacuum cleaner also has a video camera. (...) I was worried about what exactly it is filming” (I6). In addition, participants are surprised by the data streams captured by sensors: “I was recently in the health app and there are so many individual values that are tracked across the timeline that I almost wonder how all of that can be captured by just the one, two, three sensors that end up being on the watch” (I9).

The scope of data collection reflects the time and intervals at which data is collected about the smart product. All focus groups indicate that they “don't know when it’s being recorded” or that they “haven’t noticed location services are on”. Due to a habituation effect in using smart products: “I say Hey Alexa at my parents’ house, even though I only have Alexa at my house.” (I3), participants increasingly lose the feeling for when smart products record. However, as participants suspect that providers are recording continuously, some are banning their smart speakers from their private spaces, such as the bedroom.

Control of data captures the lack of information on how to restrict data collection. Participants feel that they are “more or less forced to share the data” (I9), either for the provision of the services “you just can’t avoid location tracking if you want to use certain services” or for the technical functionality: “Alexa also listens, when you turn her off. Otherwise, Alexa wouldn’t hear what I’m saying” (I9). Even with the option to disable recording, participants are not sure if recording will stop. For example, one participant notes: “Sure, Alexa has a button at the top to deactivate the microphones. But whether they are really turned off or not? Difficult to say” (I7).

Second, for data analysis, the subcategories are algorithms and visualization. Algorithms capture the absence of information on how providers improve the functionality of smart products based on algorithms or what conclusions are drawn. For example, one participant experienced when his girlfriend moved in that “Alexa suddenly noticed that a second person was using the voice assistant” (I3) and offered a voice training to remember her voice. However, the participant finds this analysis “technically creepy from a data perspective” because he was not informed beforehand. However, most participants lack the technical know-how to understand algorithms and analyses. Visualization reflects the lack of information about what analyzed data is provided to customers. Some participants question whether the full scope of the analysis will be visualized and made available to customers. They suspect, for example, that Google is withholding information beyond location history, such as personal preferences. However, many participants would like to see more “visualized data charts” (I8).

4.2. Transmission of data

The focus groups perceive hidden actions by the provider in the transmission of their data. Although participants want information about data transfer, they often lack information about device-to-device transfer, cloud transfer, and third-party transfer.

The subcategory for device-to-device transfer is API setup. This subcategory captures the absence of information about the transfer of data between smart and other personal devices. Since most participants use more than one smart product, they notice a connection of their devices, especially at home: “For example, if you have the IQ lights, they tie you completely into this whole Zigbee network” (I3). However, through the connection of their devices, the data flow to the provider is disguised: “When I turn my home pods on or off, or my smart TV, they [the providers] know all that directly as well. I think this data stream is untraceable today” (I3). In addition, participants do not know when providers gain access to the camera or apps on their smartphone by setting up APIs.

For cloud transfer, the subcategories are cloud storage and deletion. First, cloud storage captures missing information about what data is accessible and stored in clouds. Participants often desire local storage: “For me it is quite important that it just stays on the device, otherwise I would like to agree that the data may be sent to the provider” (I1). However, they do not know the extent to which their data is sent to cloud servers. For instance, one participant notes, “All this data that I thought was on my phone or on the smartwatch or somewhere, it’s just on the Garmin server somewhere. (...) Suddenly you think this whole relationship is different than I expected” (I7). But participants cannot say whether all providers have cloud servers for data storage.

Second, deletion reflects the lack of information on how customers can delete their stored data in clouds. As participants claim to have no control over data that is not stored locally on their device, they do not know if they can delete their data after it has been collected. If data is deleted when the service is terminated, participants are afraid of residual copies or backups (“How do I know my data has really been deleted if I no longer use the service”, I4). Since they are afraid that their data will not be deleted, they often ask about the security measures of the providers.

Lastly, the category third-party access includes the subcategories regulatory compliance, notice and consent, and actors. Regulatory compliance describes the lack of information whether the transfer of data complies with current data protection regulations. All focus groups agree that providers share data with third parties, though some participants are not sure what is shared “officially” and “unofficially” (I2). Particularly regarding sensitive data, participants do not know what data may be shared with third parties: “I mean, of course, we have data protection, etc., but if you take my health data now, it might be interesting to know whether it is shared legally or illegally with third parties” (I9). In addition, participants do not know if their data will be transferred to countries without GDPR requirements.

The subcategory notice and consent refers to the lack of information about when and by what means providers inform about data transfers. Focus groups are often unaware about how they get informed about the sharing of their data. Only a few have privacy policies or cookie consent banners in mind: “I think you can read about the purpose of sharing in the privacy policy, but I’m not sure” (I6). However, most participants believe that providers do not provide information in a concise manner to gain consent from customers. Thus, many participants do not know what their consent to the privacy policy refers to.

Finally, the subcategory actors reflect the lack of information about which organizations providers transfer data to and for what purposes. In the focus groups, the question of who the data is shared with was raised repeatedly. As there is “no listing by name” (I9), participants do not know the recipients to which their data is transferred. However, they suspect that not only companies, but also healthcare facilities or even their employers could receive their data. However, they lack information about the purpose of the data transfer and ask whether it is for “economic or scientific interest” (I1). Finally, participants do not know how providers grant access to their data, such as in de-anonymized or encrypted form, or “what is the person receiving my data tied to?” (I9).

4.3. Monetization of data

Participants perceive hidden actions by providers related to monetization of their data. The categories service provision and targeting describe the realization of value by providers. First, for service provision, the subcategories are value exchange, data value, and data aggregation.

Value exchange refers to the absence of information about the compensation for the disclosure of personal data. Most participants believe that their data is not only used to provide the service, but also to benefit the provider: “when you get such [smart] products into your house or buy them, you have to be aware that the data is used not only in the interest of the user, but I think also in the interest of the provider” (I1). However, participants find it difficult to determine whether the exchange of data for value is fair in terms of equal compensation. For instance, one participant notes: “(…) with the smartwatch you have put money on the table. In that sense, it’s still spying on you, even if you’ve already paid for it” (I7).

The subcategory data value captures the lack of information of what monetary value the provider attributes to personal data. Although participants are aware of the financial value of data, it is difficult for them to understand the euro amounts providers can receive for their data: “I think there is such a valuation on Facebook etc. per user, what one’s personal data is worth. But I think it is different with a smart lamp or a with a fitness watch. I think they’ve [provider] certainly retrieved some values for themselves, but I don’t think it’s possible for the end user to understand that” (I7). In addition, participants do not know “how much others pay the provider for their data” (I7).

Finally, the subcategory data aggregation captures the lack of information about specific purposes for monetizing the aggregated data. Focus groups believe that providers aggregate as much data as possible (“it’s not about the individual data point", I1), and believe "smart services help with collecting data" (I10). However, participants do not fully understand how their aggregated data will be monetized, whether, for example, to develop "customized or new services" (I5), to sell data, or for purposes yet unknown.

Second, for targeting, the subcategories are targeted advertising and targeted service. The first subcategory refers to the lack of information about the timing and use of data collected by smart products to serve targeted advertising. Focus groups describe that they feel continuously tracked by their smart devices, even when they are not actively using them. However, participants do not know when routines or preferences are collected for targeted advertising: "What I find scary, but talk myself out of, is when I think something and I get ads for exactly what I was thinking, but that can't be" (I3). Further, participants do not know at what time and on which platform they will receive targeted advertising ("The moments when it's strangest are when it hits you when you're not expecting it", I7).

Targeted services describe the lack of information about targeted services that providers create based on data collected by smart products. Although focus groups believe that targeted services are created, such as targeted risk premiums by health or car insurers, they do not know the full scope of targeted services. In addition, they fear that targeting does not reflect their true behaviors or preferences. For instance, regarding the maintenance behavior of a smart vacuum cleaner, one participant notes "maybe the software ultimately decides, I'm less careful with my appliance and thus it will break down six months earlier, although this is not true" (I6). Finally, participants do not know how providers know the relevant players: "The [smart] car manufacturer does not know where I am insured, he would have to write to all insurance companies on the market and then sell the data" (I2).

5. Discussion

In this study, we aimed to investigate customer perceptions of hidden actions by smart product providers. We discerned three perceived hidden actions, representing a form of information asymmetry within online exchange relationships. Agency theory posits that hidden actions can create an informational advantage for the agent (Eisenhardt, 1989). Building upon agency theory, we integrated the concept of hidden actions into B2C service ecosystems, as depicted in Figure 2. This allowed us to achieve a comprehensive understanding of the information asymmetries within provider-customer relationships in the realm of smart products. While prior IS studies in the context of online marketplaces have traditionally conceptualized principal-agent situations as transactional arrangements involving two parties under uncertainty (e.g., Pavlou et al., 2007), our research focuses specifically on the provider-customer relationship within smart service ecosystems. Providers, by serving as facilitators of platforms for service exchange, orchestrate these ecosystems, while customers contribute to the creation of services through data sharing (Lusch & Nambisan, 2015; Herterich et al., 2023; Vargo, 2008; Gawer, 2022). To co-create the core value of smart services, providers and customers engage in two transactional arrangements (Eisenhardt, 1989). First, customers (principals) delegate the delivery of a smart product to the provider (agent) and make a payment in return. These smart products serve as the technological foundation for realizing smart services (Adner, 2017; Beverungen et al., 2019). The value of smart services is unlocked through the use of information, such as fitness management based on analyzed health data (Lim et al., 2018; Lusch & Nambisan, 2015). Thus, the second transaction pertains to the exchange of personal data in return for value derived from its use.

Uncertainty arises when sellers possess an informational advantage about their actions that buyers perceive as hidden (Mishra et al., 1998). In the context of ecosystems, where various actors engage in value creation activities (Adner, 2017), customers perceive three actions related to data handling as hidden. The first perceived hidden action concerns data processing. Customers lack information about how smart products collect and analyze their data as data processing relies on the sensory and analytical components of these products (Porter & Heppelmann, 2014). This uncertainty extends to the continuous collection of data by sensors (Cichy et al., 2021), leaving customers in the dark about the nature, volume, and timing of the data, as well as their control over it. The second perceived hidden action relates to data transmission, with customers perceiving strong regulation by providers. This view is consistent with the control of data exchange by the ecosystem orchestrator as a "private regulator" (Gawer 2022, p. 112). Thus, customers feel they have less information than providers about APIs facilitating data transfers between smart devices and personal devices, data storage in clouds, or the entities involved in data sharing. The last perceived hidden action involves the monetization of personal data. While customers are aware that their data is exchanged for smart services or value derived from its use, they perceive they often lack information about what constitutes a fair exchange or the monetary value of their data. This lack of transparency can lead to customer dissatisfaction,

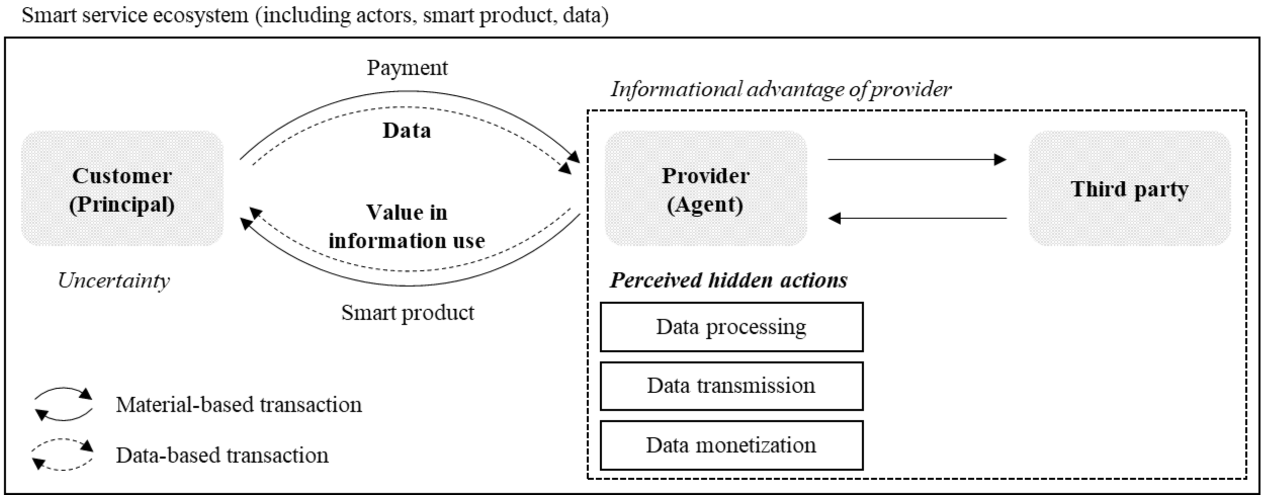

Figure 2. Perceived hidden actions in smart service ecosystems.

particularly when their perceived net value is lower than what providers gain (Wagner et al., 2021). Smart services can be monetized through data or direct payments (Paukstadt et al., 2019). Nevertheless, customers feel that they are insufficiently informed about the extent of data monetization, such as for targeted advertising or additional services.

In summary, customers often perceive knowledge gaps about providers' data processing, transmission, and monetization, leading to inherent information asymmetries in smart service ecosystems (Eisenhardt, 1989). Agency theory suggests that these gaps go beyond customers' reluctance to engage with privacy policies (Acquisti et al., 2020). Providers, driven by the pursuit of data monetization, might engage in actions to hide information or evade privacy regulations to advance their self-interests. This opportunistic behavior can be notably affected by diverse business models, particularly advertising-based models that provide significant incentives to keep data usage hidden from users (Gawer, 2022). However, it is vital to recognize that not all service providers seek to mislead or withhold information. Transparency in practices, especially regarding data protection, can be a unique selling point, as trust plays a pivotal role in data disclosure (Smith et al., 2011). Lastly, the ecosystem dynamics extend beyond the customer-provider relationship to include other actors in co-creating value from data (Herterich et al., 2023). However, our findings demonstrate that customers often lack awareness of the involvement and roles of third parties (Adner, 2017). Thus, transactional agreements between providers and third parties can create an additional informational advantage to providers.

6. Theoretical and practical contribution

The primary objective of this study was to investigate individuals' perceptions of hidden actions. To the best of our knowledge, no prior research has investigated which actions of smart product providers are perceived as hidden by customers. We empirically show that customers perceive three hidden actions. Drawing on agency theory, we find that the relationship between smart product providers and customers is characterized by information asymmetries resulting from the hidden actions. Our results are valuable for research and practice.

First, our results contribute to the current debate about uncertainty in privacy decisions (e.g., Acquisti et al., 2018, 2020; Al-Natour et al., 2020; Trzaskowski, 2022). Information asymmetries distort understanding of data handling and prevent customers from assessing privacy risks and making informed and rational decisions (Trzaskowski, 2022; Al-Natour et al., 2020). We identified three hidden actions of providers that may shed light on privacy risks and guide future research to address the need for transparent privacy tradeoffs and clearer policies (e.g., Acquisti et al., 2018; Liu et al., 2022). Our findings can facilitate effective transparency (Tsai et al., 2011; Trzaskowski, 2022). Moreover, we draw on agency theory to comprehend the significance of hidden actions within smart service ecosystems (Eisenhardt, 1989). Thereby, we expand existing uncertainty mitigation models rooted in agency theory (e.g., Pavlou et al., 2007; Chang & Chen, 2014; Al-Natour et al., 2020). In this context, we unbundled a data-based transaction and a materials-based transaction between smart product providers and customers.

Consistent with prior findings, we emphasize that customers' uncertainties in using digital goods or services are primarily due to hidden actions in handling their data (e.g., Al-Natour et al., 2020).

Second, we contribute to the evolving theoretical understanding of ecosystems (Oliveira, 2019). We extend the concept of smart service ecosystems to the consumer context (Lusch & Nambisan, 2015; Herterich et al., 2023). We provide an understanding of actors, information flow, and value creation in these ecosystems (Adner, 2017). Drawing from IS privacy literature, we reveal that ecosystem activities often remain concealed from customers, obscuring risks of data disclosure. Since data is a key resource in digital platforms and ecosystems (Gawer, 2022), we encourage further research on data practices that consider the dual roles of data in privacy and monetization (Burmeister et al., 2021; Kurtz et al., 2018).

In terms of practical contributions, we address customers, providers, and legislators. First, we raise customer awareness regarding the hidden actions of service providers. As these actions pose privacy risks, customers are empowered to make more informed and rational decisions about their privacy. Second, providers can nudge customers into revealing their data through dark privacy patterns, masking the adverse consequences (Gawer, 2022). However, past privacy scandals have shown that customer trust is fragile, leading many to switch providers. Effective ecosystem governance entails creating value for stakeholders despite divergent interests. Providers can reduce fear of opportunistic behavior and strengthen trust by disclosing relevant information about their actions, allowing customers to weigh data-related risks and benefits. Finally, this study can guide legislators in developing privacy tools to reduce information asymmetry. However, it is important to recognize that customers, providers and third parties have a common interest in creating mutual benefit. Thus, tools should enable informed privacy decisions by customers while allowing ecosystem stakeholders to leverage mutual value of data.

7. Limitations and further research

Our study has some limitations that offer directions for future research. Firstly, the scope of hidden actions we analyzed may be limited by actions not foreseeable by customers, potentially due to limited data science literacy. However, the use of focus groups for exploring privacy-related theoretical constructs provides opportunities for more in-depth investigations in subsequent studies (Karwatzki et al., 2017). Second, the generalizability of our results may be limited as we focused on B2C customers in Europe. Exploring insights from different cultural contexts, such as the U.S. or China, or examining B2B settings, could provide a more comprehensive understanding. Hidden actions might also vary based on specific service providers' business models; some prioritize data selling, while others focus on enhancing services. Further studies could delve into context-specific hidden actions, such as those in social media (Chang & Chen, 2014) or B2B services. Third, assessing the principal-agent dynamics within B2C service ecosystems empirically and extending involvement to additional stakeholders is necessary. Existing models for mitigating uncertainty could be refined based on the identified hidden actions by exploring their impact on information asymmetry and uncertainty (e.g., Pavlou et al., 2007). Additionally, investigating the effectiveness of information or trust signals in reducing asymmetric information due to the identified hidden actions is valuable. Exploring alternative signaling mechanisms to address asymmetric information in these actions holds promise for future research. Lastly, acknowledging the inherent limitations of qualitative-exploratory research, we have prioritized transparency and replicability in both our findings and categories (Gioia, 2013).

8. References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2018). *The Cambridge handbook of consumer privacy*. Cambridge University Press.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. Journal of Consumer Psychology, 30(4), 736-758.

Adner, R. (2017). Ecosystem as structure: An actionable construct for strategy. Journal of Management, 43(1), 39-58.

Al-Natour, S., Cavusoglu, H., Benbasat, I., & Aleem, U. (2020). An empirical investigation of the antecedents and consequences of privacy uncertainty in the context of mobile apps. Information Systems Research, 31(4), 1037-1063.

Beverungen, D., Müller, O., Matzner, M., Mendling, J., & Vom Brocke, J. (2019). Conceptualizing smart service systems. Electronic Markets, 29, 7-18.

Bourreau, M., Caffarra, C., Chen, Z., Choe, C. C., Crawford, G., Duso, T., Genakos, C., Heudues, P., Peitz, M., Rønde, T., Schnitzer, M., Schutz, N., Sovinsky, M., Spagnolo, G., Toivanen, O., & Valletti, T. (2020). Google/Fitbit will monetise health data and harm consumers (CEPR Policy Insights No. 107). Centre for Economic Policy Research.

Burmeister, F., Kurtz, C., Vogel, P., Drews, P., & Schirmer, I. (2021). Unraveling privacy concerns in complex data ecosystems with architectural thinking. 42nd

International Conference on Information Systems, Austin, Texas, USA.

Chang, L., & Chen, J. V. (2014). Aligning principal and agent's incentives: A principal–agent perspective of social networking sites. Expert Systems with Applications, 41(6), 3091-3104.

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), 1863-1889.

Corbin, J., & Strauss, A. (2008). Basics of qualitative research*: Techniques and procedures for developing grounded theory* (3rd ed.). Thousand Oaks, CA: Sage.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. Academy of Management Review, 14(1), 57-74.

Fern, E. F., & Fern, E. E. (2001). *Advanced focus group research*. Sage.

Frier, S. 2018. Facebook Says There May Be More Cambridge Analytica-Sized Leaks. https://www.bloomberg.com/news/articles/2018-04-26/facebook-saysthere-may-be-more-cambridge-analytica-sized-leaks

Gawer, A. (2022). Digital platforms and ecosystems: Remarks on the dominant organizational forms of the digital age. Innovation, 24(1), 110-124.

GDPR. (2016) General Data Protection Regulation – Regulation (EU) 2016/679 of the European Parliament and of the Council, Official Journal of the European Union (111).

Gerlach, J., Widjaja, T., & Buxmann, P. (2015). Handle with care: How online social network providers' privacy policies impact users' information sharing behavior. The Journal of Strategic Information Systems, 24(1), 33-43.

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. Organizational Research Methods, 16(1), 15-31.

Herterich, M. M., Dremel, C., Wulf, J., & vom Brocke, J. (2023). The emergence of smart service ecosystems – The role of socio-technical antecedents and affordances. Information Systems Journal, 33(3), 524-566.

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

Kitzinger, J., Qualitative research. Introducing focus groups. British Medical Journal, 311(7000), 299-302.

Knote, R., Janson, A., Söllner, M., & Leimeister, J. M. (2020). Value co-creation in smart services: A functional affordances perspective on smart personal assistants. Journal of the Association for Information Systems, 22(2), 418-458.

Kurtz, C., Semmann, M., & Schulz, W. (2018). Towards a framework for information privacy in complex service ecosystems. 39nd International Conference on Information Systems, San Francisco, USA.

Lim, C., & Maglio, P. P. (2018). Data-driven understanding of smart service systems through text mining. Service Science, 10(2), 154-180.

Lim, C., Kim, K. H., Kim, M. J., Heo, J. Y., Kim, K. J., & Maglio, P. P. (2018). From data to value: A nine-factor framework for data-based value creation in information-intensive services. International Journal of Information Management, 39, 121-135.

Liu, B., Pavlou, P. A., & Cheng, X. (2022). Achieving a balance between privacy protection and data collection: A field experimental examination of a theory-driven information technology solution. Information Systems Research, 33(1), 203-223.

Lusch, R. F., & Nambisan, S. (2015). Service innovation. MIS Quarterly, 39(1), 155-176.

Mishra DP, Heide JANB, Cort SG (1998) Information asymmetry agency and levels of relationships. Journal of Marketing Research, 35(3), 277–295.

Parvinen, P. (2020). Advancing data monetization and the creation of data-based business models. Communications of the Association for Information Systems, 47(1), 2.

Paukstadt, U., Strobel, G., & Eicker, S. (2019). Understanding services in the era of the internet of things: a smart service taxonomy. 27th European Conference on Information Systems, Stockholm & Uppsala, Sweden.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. MIS Quarterly, 31(1), 105-136.

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

S. Oliveira, M. I., Barros Lima, G. D. F., & Farias Lóscio, B. (2019). Investigations into data ecosystems: a systematic mapping study. Knowledge and Information Systems, 61, 589-630.

Saldaña, J. (2021). *The coding manual for qualitative researchers* (4th ed.). Sage.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. MIS Quarterly, 35(4), 989-1015.

Trzaskowski, J. (2022). Data-driven value extraction and human well-being under EU law. Electronic Markets, 32(2), 447-458.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. Information Systems Research, 22(2), 254-268.

Vargo, S. L. (2008). Customer integration and value creation. Journal of Service Research, 11(2), 211-215.

Wagner, A., Wessels, N., Brakemeier, H., & Buxmann, P. (2021). Why free does not mean fair: Investigating users' distributive equity perceptions of data-driven services. International Journal of Information Management, 59, 1023-1036.

Warkentin, M., Goel, S., & Menard, P. (2017). Shared benefits and information privacy: What determines smart meter technology adoption?. Journal of the Association for Information Systems, 18(11), 759-786.