Received: 11.05.2022 | Revised: 29.05.2023 | Accepted: 22.12.2023

Smart Wearables as Silent Witnesses: Privacy Concerns versus Possible Legal Advantages

*Melina Schleef, Sabine Gless, Christian Stummer**

Summary: Many smart wearables can collect personal movement data and use these data to provide personalized services. However, data storage may cause privacy concerns among consumers. Thus, when deciding whether to equip their products with such an ability or refrain from doing so, managers must consider potential backfire due to the possibly strong opinions of customers regarding their privacy. While prior studies have shown that benefits of smart products that can be experienced on a regular basis (e.g., more convenience in accomplishing daily routines) can outweigh data privacy concerns, we investigate whether this is also true for a feature of a smart wearable that is of use only in a rare event (or even never). The respective application case is a smart wearable serving as a silent witness that might play a role when being in need of a proof of exoneration (e.g., that its wearer has not been present at a certain crime scene at the time of an alleged offense). Furthermore, we study the difference between customers being directly affected (as the wearer of a smart wristband) or indirectly affected (as the owner of a dog with a smart dog collar).

Keywords: smart wearables, movement data, privacy concerns, evidence in legal proceedings, consumer behavior, experimental research

Smart Wearables als stille Zeugen: Datenschutzbedenken versus mögliche rechtliche Vorteile

Zusammenfassung: Smart Wearables können persönliche Bewegungsdaten sammeln und damit personalisierte Services anbieten. Die Speicherung von Daten kann jedoch bei Konsumenten Datenschutzbedenken auslösen. Daher müssen Manager abwägen, ob sie ihre Produkte mit entsprechenden Funktionalitäten ausstatten oder lieber darauf verzichten, weil Konsumenten angesichts von starken Privatsphäre-Vorbehalten vom Kauf absehen könnten. Während bisherige Studien gezeigt haben, dass ein regelmässig erlebter Mehrwert durch die smarten Services (z.B. mehr Bequemlichkeit bei alltäglichen Erledigungen) die Datenschutzbedenken überwiegen kann, untersuchen wir, ob dies auch zutrifft, wenn der Service eines Smart Wearable nur in seltenen Fällen (oder auch nie) gebraucht wird. Als Anwendungsfall dient ein Smart Wearable als „stiller Zeuge“, der eine Rolle spielen kann, wenn ein entlastendes Beweismittel benötigt wird (z.B.,

* **Corresponding Author**: Christian Stummer, christian.stummer@uni-bielefeld.de.

dass der Träger zum Zeitpunkt eines Verbrechens nicht am Tatort war). Des Weiteren untersuchen wir, ob es einen Unterschied macht, ob der Konsument direkt (als Träger eines smarten Fitness-Armbands) oder indirekt (als Besitzer eines Hundes mit smartem Hundehalsband) betroffen ist.

Stichwörter: Smart Wearables, Bewegungsdaten, Datenschutzbedenken, Beweismittel in Gerichtsverfahren, Konsumentenverhalten, Experimentelle Forschung

1. Introduction

In the last decade, market diffusion and usage of smart consumer products have been on the rise due to the advancement of technology and the increasing availability of network services. Accordingly, numerous day-to-day objects have evolved that provide new digital services (e.g., bathroom scales, light bulbs, or cars). Smart wearables, which can be worn on the body, are a prominent example of such objects and have a market that is projected to grow from USD 95 billion in 2022 to USD 383 billion by 2032 (GlobeNewswire 2023). Consequently, smart wearables are receiving increased attention from both researchers and practitioners who are interested in the drivers of and barriers to product adoption.

Our work contributes to the respective stream of research by investigating the trade-off consumers make regarding privacy concerns and the possible benefits of privacy-intruding features of certain smart products—that is, we are working in the realm of privacy calculus theory (see, e.g., Culnan and Armstrong 1999). Specifically, we examine the ability of smart wearables to store movement (geo-tracking) data as a means of obtaining alibi evidence in possible criminal proceedings. It is noteworthy that authorities already exploit data from wearables in prosecuting crimes (e.g., Altimari 2018), and that experts expect that data from wearables have substantial potential as evidence in criminal investigations and prosecutions in the United States (Rodis 2020, Steele 2022) as well as in Germany (Fährmann 2020) and Switzerland (Gless and Stagno 2018). Although the data being used so far are not geo-tracking data (but arm movement data or certain medical data), it seems likely that tracking data will play a role in this respect once it is more widely available. It should also be noted that in all jurisdictions, information generated by devices used by defendants or victims can be proffered as evidence to exonerate or incriminate.

Besides referring to a novel service of smart wearables, the application case offers research insights in two respects. First, prior studies have already indicated that proper services of smart products that can be experienced on a regular basis, such as higher convenience provided by a robot vacuum cleaner, can mitigate privacy concerns (e.g., Shaw and Sergueeva 2016; Princi and Krämer 2020; Jabbar et al. 2023). This finding also seems to hold true for services that could be expected to be useful once in a while, such as the emergency detection capability of a robot vacuum cleaner (Schleef et al. 2022). However, it has not yet been investigated whether consumers are willing to override their data privacy concerns even for the sake of a benefit that nearly none of them will ever realize, such as the need to use geographical movement data as exculpatory (alibi) evidence when being suspected to have committed a certain crime. The answer to this question is even more open in countries like Germany, where privacy concerns are particularly prevalent and data protection is a highly sensitive topic (Statista 2015, 2022a). Second, we expect an effect—analogous to child–caregiver attachment theory—depending on who is perceived to possibly suffer consequences from being falsely accused and being in need

of speculative alibi evidence—that is, is it the customer themselves or somebody to whom they are emotionally bonded and take care of (e.g., their beloved dog).

To explore the above research questions, we performed two experimental studies. In our first study, we used a smart wristband to test the expected main effect—that is, whether there is a difference in consumer purchase intention between (i) a smart wristband that does not store movement data, (ii) a smart wristband that stores movement data for later general usage (e.g., for training purposes), and (iii) a smart wristband that also has the ability to store movement data that may be used as evidence in legal proceedings. To dig deeper into the findings, we also tested privacy concerns and confidence in court hearings as possible mediators. In the second study, we replicated the first study with a different wearable—that is, a smart dog collar.

The research contribution of our work is fourfold. First, we apply privacy calculus theory to an innovative use case—that is, storing geographical movement data collected by a smart wearable in favor of the wearers in possible legal proceedings. While today such a benefit in the legal context is probably not familiar for most consumers, it will increase in relevance with more wearables coming to the market in the future. Second, this application case is special as it offers a benefit that will only be realized in very rare cases and only for a few customers. Third, we study whether the difference in purchase intention depends on who might gain an advantage from the offered service (i.e., the customers themselves or their dogs). Fourth, our results can be valuable for innovation managers who are responsible for the development and market introduction of smart wearables.

The remainder of this paper is organized as follows. Section 2 gives an overview of smart products in general and smart wearables in particular, and it introduces the two mediators we have accounted for—privacy concerns and confidence in court hearings. Sections 3 and 4 describe the two experimental studies with respect to the hypotheses, study design, and results. Section 5 discusses the theoretical and managerial implications of the findings. Section 6 lists the remaining limitations and provides an outlook to promising directions for further research.

2. Background

Although there is no consensus on the definition of smart products (for a systematic review, see Raff et al. 2020), it is widely acknowledged that smart products are cyber-physical devices that have both tangible and intangible components. The tangible ones specify the material ("physical") nature of a smart product, while the intangible ones determine the smart product's software-based ("cyber") digital capabilities. Obviously, the latter components are key for rendering smart services and operating within a larger ecosystem. In an attempt to seize the term "smart products," which otherwise buzzes around among academics and practitioners, Raff et al. proposed a framework featuring four different archetypes of smart products, which build on each other. In this framework, digital products constitute the basic type (i.e., all smart products are digital), followed by connected products, responsive products, and—as the most sophisticated type—intelligent products.

The business impact of smart products can hardly be overestimated, as they have led to the transformation of both companies and competition (Porter and Heppelmann 2014, 2015). This ongoing process brings along various opportunities and challenges due

to the formation of new business models, new distribution channels, and new business ecosystems (Dawid et al. 2017; Kaiser and Stummer 2020; Hanelt et al. 2021; Langley et al. 2021). Recent progress in integrating advanced AI-based functionality into smart products will further accelerate this process. Examples of forthcoming applications of AI in smart wearables are described by Nahavandi et al. (2022).

Within the larger group of smart products, the above-mentioned smart wearables represent a broad category of devices worn on the body. These devices are able to collect user information and, more often than not, are connected to a network in order to transmit data and communicate with other devices or applications (Nascimento et al. 2018; Oh and Kang 2021). If smart wearables provide location-based services, such as in our application cases, they can be categorized as responsive products; in the future, wearables might even fall into the category of intelligent products (i.e., once they offer complex context-based services and learn from the interaction with the wearers, improve their services, anticipate events, and make decisions). Several (sub-) streams of research have focused on smart wearables—regarding, for example, the diffusion of smart wearables in complex and dynamic environments (e.g., Zhan et al. 2022), the use of smart wearables in health care (e.g., in the prevention diagnosis and the management of cardiovascular disease; Bayoumy et al. 2021), or design features that influence the continued use of smart wearables (e.g., El-Gayar et al. 2021). Although smart wearables are products, prior studies have discussed them in the context of Internet-of-Things (IoT) services or devices (e.g., Decker and Stummer 2017).

Thus far, a substantial body of literature has investigated the drivers of, as well as the barriers to, the adoption and usage of smart products. In many of these studies, consumers' privacy concerns play a prominent role (e.g., Michler et al. 2022; Schleef et al. 2022; Schomakers et al. 2022). Privacy, described as the right to be let alone, refers to personal information that has multiple dimensions: privacy of an individual's body, privacy of personal behavior, privacy of personal communication, and privacy of personal data (Clarke 1999; Luo 2002). Regarding the latter, the General Data Protection Regulation (GDPR) states that "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." This definition comprises the movement data of an identifiable natural person. The storage of such movement data can raise concerns when consumers suspect the secondary use of their personal information and perceive this as an intrusion into their privacy (Mani and Chouk 2019). With respect to smart (health) wearables, the most relevant aspects of privacy concerns appear to be perceived data sensitivity, perceived data variety, and perceived tracking activity (Becker et al. 2017). In this line of research, Paul et al. (2020) investigated how privacy policies can reduce the privacy concerns of users of a hypothetical fitness wearable, and Psychoula et al. (2020) studied privacy risk awareness in wearables and the IoT.

In a lesser-known field of application, the compilation of movement profiles by means of smart wearables could play a role in criminal proceedings, for example, when law enforcement needs to scrutinize a suspect's movement or when a suspect wishes to present an alibi. So far, the usage of data taken from smart wearables has already become part

of the technology toolbox of law enforcement experts and has been used for conviction (e.g., Hauser 2017, 2018), albeit the officials have typically not used geodata but data from a smart wristband indicating arm movements and certain medical data. In the United States, data generated by a wearable has led to high-profile criminal cases in which such information was used to exonerate defendants. For example, a defendant presented Fitbit data proffering that he had been at home and asleep at the time his girlfriend had been killed (Briquelet, 2017). Moreover, Kendall (2019) describes how authorities use data from wearable fitness trackers to confirm or deny victims' stories regarding alleged attacks. In Germany and Switzerland, as in other civil law countries, where courts are required to establish the truth, all evidence relevant for fact-finding must be considered. This includes tracking (movement) data, which can work in both ways—that is, in favor of or against a suspect and, accordingly, could also be perceived as risk (i.e., that authorities might seize the data). However, a guilty person would probably not offer incriminating movement data that is saved on one's own device, but a suspect claiming innocence would be more than happy to provide data if such exculpatory evidence is available and could be presented before the court as corroborating evidence of an alibi. In the latter case, a smart wearable collecting tracking data could serve as a silent witness and support its wearer's statement that they were not present at the site of crime at the time of the offense. As stated above, information generated by wearables has already been used to exonerate and incriminate defendants, as has the use of other data produced by devices in the possession of a victim or defendant, such as biometric data on a pacemaker, GPS signals, or recordings from smart-home devices (Steele 2022). The way in which such data are used in different jurisdictions depends on their respective approach to determining its relevance for the facts to be proven, its validity for the evidentiary question ("Does the method in fact measure what it purports to measure?"), and its reliability ("Does it do so accurately?"). Data from a fitness tracker, such as Fitbit, and data generated by other devices will fulfill their potential when a robust taxonomy for its use as evidence in criminal proceedings is established (for a more in-depth discussion, see Silverman et al. 2024). While the evidentiary details in a criminal proceeding have to be assessed in each individual case, the confidence of the owner of the smart wearable of being able to rely on such a smart silent witness may have an impact on their expectation of procedural justice (i.e., assessment that a procedure is fair; Wallace and Goodman-Delahunty 2021) and outcome satisfaction (i.e., being pleased with the judgment of a court hearing; Poythress et al. 2002), thereby increasing the wearer's confidence in court hearings (Poythress et al. 2002).

On the bottom line, consumers weigh the risks of data disclosure and the value proposition of the smart wearable under consideration. The corresponding decision-making process is addressed in privacy calculus theory (Laufer and Wolfe 1977; Culnan and Armstrong 1999), which has been applied in numerous fields. For example, the privacy implications of location-based services—as in our case—were studied by Naous et al. (2019), who found that there is a need for transparent control settings, users are willing to disclose for monetary incentives, and they are not cognizant about interdependent privacy risks. Furthermore, the extent to which privacy information is willingly provided depends on the provided service: Kim et al. (2019) found that consumers do not pay much attention to perceived privacy risk when better personalized services in the smart home or for smart transportation are promised; however, with respect to healthcare services,

they are considerably more sensitive and, thus, less willing to provide their personal information. Moreover, research also showed that consumers' willingness to share data can be influenced by affective states (Kehr et al. 2015), which nicely relates to our expectation that the attachment to their dogs has an effect on the dog owners' purchase intentions for a smart dog collar providing a functionality that could be of help for the dog when necessary (the reasoning is analogous to child–caregiver attachment theory by Bowlby 1969). Regarding wearables, prior studies applying privacy calculus theory were performed by Li et al. (2016) for healthcare wearables and Gao et al. (2015) for fitness wearables. Both were concerned with wearables that provide their benefits on a regular basis, and in both cases, it was found that the subjects cared about perceived privacy risk in their adoption decision.

3. Experimental Study 1

3.1 Hypothesis Development

The hypotheses for our experimental study rest on privacy calculus theory. In light of previous research, which often concludes that consumers are willing to override their privacy concerns even for small benefits (e.g., Kim et al. 2019; Princi and Krämer 2020), we assume that this also holds true for regular wearables. Correspondingly, having access to one's movement data for future usage—regardless of whether the benefit is advertised only in a generic way or also for the specific purpose investigated in our use case—should increase consumers' purchase intentions:

Hypothesis 1: Advertising the storage of movement data providing access for future usage increases consumers' purchase intentions of the smart wearable.

To dig deeper and learn about the effect of a feature that can be realized only in rare events (if so at all), we differentiate between the general (regular) usage of movement data collected by a smart wearable (e.g., for compiling training statistics) and the specific usage as a silent witness being advertised as an additional benefit. In the first hypothesis from a set of three related hypotheses, we assume that already the provision of movement data that can be utilized in general use cases (i.e., without mentioning the silent witness functionality) increases consumers' purchase intentions:

Hypothesis 2a: Advertising the storage of movement data providing access for general future usage increases consumers' purchase intentions of the smart wearable.

According to privacy calculus theory, increasing the benefits by adding a feature (i.e., the alibi functionality) while there is no change regarding privacy concerns should not have a negative effect. Therefore, in light of our expectation regarding Hypothesis 2a, we can expect that equipping the smart wearable with the silent witness functionality, which provides users with an alibi in the event of legal proceedings against them (given that they claim to be innocent), also increases purchase intentions compared to not saving movement data:

Hypothesis 2b: Advertising the storage of movement data providing access for future usage to serve as alibi or exculpatory evidence in legal proceedings increases consumers' purchase intentions of the smart wearable.

Furthermore, we assume that the alibi functionality—although it may be realized only in very rare instances—has value added because of the potential harshness of consequences when an alibi is needed but not available. This benefit might result in Hypothesis 2b being supported while Hypothesis 2a being rejected, and even if both hypotheses would be supported, the benefit from the alibi functionality should have a noticeable positive effect on purchase intention compared with an otherwise identical smart wearable that does not provide this functionality. Therefore, we formulate the following hypothesis:

Hypothesis 2c: Advertising the storage of movement data providing access for future usage also to serve as alibi or exculpatory evidence in legal proceedings increases consumers' purchase intentions of the smart wearable more than just advertising the storage of movement data providing access for general future usage.

To better understand the underlying (implicit) reasoning, we account for two mediators. Obviously, we include data privacy concerns as the first potential mediator. If consumers are indeed concerned about the misuse of the movement data collected by the smart wearable, these increased concerns should have a negative effect, attenuating their intentions to purchase the product. As a second potential mediator, we include confidence in court hearings, which comprises the expectation of procedural justice, outcome satisfaction, and trust in the court's future actions and performance (Poythress et al. 2002; Wallace and Goodman-Delahunty 2021). This benefit is expected to increase when movement data collected by the smart wearable are available to be used as alibi evidence in legal proceedings, and thus, it should strengthen purchase intentions. Accordingly, we formulate the following hypotheses:

Hypothesis 3a: By increasing data privacy concerns, advertising the storage of movement data providing access for future usage attenuates consumers' purchase intentions of the smart wearable.

Hypothesis 3b: By increasing perceived confidence in court hearings, advertising the storage of movement data providing access for future usage increases consumers' purchase intentions of the smart wearable.

3.2 Study Design

Procedure. Our study was a between-subjects experiment in which participants were randomly assigned to one of three groups. Participants were asked to put themselves in a situation of looking for a smart wristband, and all were shown the same smart wristband. However, the description of the movement data usage of the smart wristband differed between the three settings. In the first setting (Scenario A), the smart wristband collects but does not save data so that no one has access to this data afterward. In the second setting (Scenario B), the smart wristband collects and saves data in the app for future usage (without further specification). In the third setting (Scenario C), the smart wristband collects and saves data in the app for future usage, and it is suggested that these data can be used as alibi or exculpatory evidence in possible legal proceedings.

The product as well as its provider "YouTrack" were fictitious. In a pretest with 80 participants, we tested several alternatives for the provider's name and ultimately selected the above-mentioned one, as it was perceived as particularly realistic and appealing by the participants in the pretest. In the same pretest, we also tested alternative pictures of

running couples as well as color schemes to be used in the advertisement and, again, selected the most realistic and appealing one.

Procedurally, the participants in the main study began by reading the scenario description, which contained information regarding the smart wristband. Furthermore, they saw a corresponding advertisement (see Fig. 1), in which the following manipulations are included in a footnote: *"The collected movement data is not saved. Hence, no one has access to this data afterwards"* in Scenario A, *"The collected movement data are saved locally in the app. Hence, you have access to this data for future usage if needed"* in Scenario B, and *"The collected movement data are saved locally in the app. Hence, you have access to this data for future usage, if needed. Especially, in case of suspicion of a criminal act, movement data can serve as alibi or exculpatory evidence in legal proceedings"* in Scenario C. Then, the participants responded first to items referring to the dependent variable (i.e., purchase intention), second to the mediators (i.e., data privacy concerns and confidence in court hearings), third to manipulation and realism checks, and fourth to personal information. It must be noted that the product description and the questionnaire were in German (and were translated for this paper), as both of our experimental studies were conducted in Germany.

Figure 1: Advertisements Used in Study 1

Sample. Participants were referred to our questionnaire through the panel provider *Bilendi* (www.bilendi.de) at the beginning of February 2023. The provider guaranteed that all participants were athletic, from Germany, and at least 18 years of age, and also assured us that the sample was representative of the population in Germany with respect to age and gender. However, small discrepancies from official statistics occurred due to the ex-post exclusion of certain responses, which happened when participants failed to correctly answer attention checks (e.g., *"Please now tick the 'strongly disagree' box"*), when we found highly unusual patterns in response behavior (e.g., ticking the same answer on the scale for most questions), or when we identified unusual response times (e.g., extraordinarily long or short response times or very long pauses between some of the answers given). In all 18 instances of responses that were excluded, several of the above issues were found.

The final sample contained responses from 312 participants (48.7% female; M_{age} = 44.12; SD = 14.4).

Measures. First, we measured purchase intention as the dependent (outcome) variable. To this end, we used three items, each on a 7-point scale ranging from "1 = strongly disagree" to "7 = strongly agree". It should be noted that we used this same scale for all items in our questionnaire. The items for purchase intention were adapted from Fuchs et al. (2015): *"It is likely that I would buy YouTrack's smart wristband"*; *"I would feel good about buying YouTrack's smart wristband"*; and *"I would definitely buy YouTrack's smart wristband"* (α = 0.954; AVE = 0.849; CR = 0.944). To avoid unintended priming effects of the mediators on the outcome variable, we measured the mediators only afterwards. For measuring data privacy concerns, we used three items on our 7-point scale; the items were adapted from Bleier and Eisenbeiss (2015): *"It bothers me that YouTrack is able to collect my data"*; *"I am concerned that YouTrack has too much data about me"*; and *"I am concerned that YouTrack could use my data in ways I cannot foresee"* (α = 0.938; AVE = 0.873; CR = 0.954). We measured confidence in court hearings as the second mediator by means of four items on the 7-point scale; these items were adapted from Poythress et al. (2002), and all of them began with *"In case of an incidence when wearing YouTrack's smart wristband, […]"* and ended with either *"I would feel better in a subsequent court hearing"*; *"I would be less upset in a subsequent court hearing"*; *"I would feel safer in a subsequent court hearing"*; or *"I would be more hopeful in a subsequent court hearing"* (α = 0.958; AVE = 0.836; CR = 0.953). Finally, we asked for personal information, such as gender and age.

3.3 Results

Manipulation and realism checks. The item *"The scenario description said that the collected movement data are not saved. Hence, no one has access to this data afterwards"* was implemented as a first manipulation check. The results of this check indicated that our manipulation was successful, as the mean M_{no_data} of responses referring to the group of participants from Scenario A, who received the information that collected movement data is not saved so that no one has access to this data afterwards, was significantly higher than the mean of responses $M_{data\_storage/legal\_usage}$ from the participants from the unified Scenarios B and C, who were told that the collected data is saved so that the user has access to this data for future usage (M_{no_data} = 5.13, $M_{data\_storage/legal\_usage}$ = 3.18; $F_{1,310}$ = 75.659, $p < 0.001$). The second manipulation check *"The scenario description said that the collected movement data is saved locally in the app. Hence, you have access to this data for future usage if needed"* confirmed this indication as the mean of responses referring to participants from Scenario A was significantly lower than the mean of responses from Scenarios B and C ($M_{data\_storage/legal\_usage}$ = 5.40, M_{no_data} = 4.15; $F_{1,310}$ = 36.675, $p < 0.001$). A third manipulation check *"The scenario description said that the collected movement data is saved locally in the app. Hence, you have access to this data for future usage, if needed. Especially, in case of suspicion of a criminal act, movement data can serve as alibi or exculpatory evidence in legal proceedings"* revealed a significant difference between participants from Scenario C and those from Scenarios A and B ($F_{2,309}$ = 28.635, $p < 0.001$). Planned contrasts indicated higher means for participants from Scenario C in comparison to participants from Scenario A (M_{legal_usage} = 5.02, M_{no_data} = 3.07; $F_{1,309}$ = 55.643, $p < 0.001$) and participants from Scenario B (M_{legal_usage} = 5.02, $M_{data\_storage}$ = 3.65;

$F_{1,309}$ = 25.490, p < 0.001). Finally, a realism check using three items (*"The described situation seems to be realistic"*; *"It was easy to put oneself in the described situation"*; and *"The scenario was easy to understand"*) confirmed that the situation was perceived as realistic (M = 5.00; SD = 1.29).

Hypothesis 1. An ANCOVA indicated that participants from Scenarios B and C have higher purchase intentions than participants from Scenario A ($M_{data\_storage/legal\_usage}$ = 4.09, M_{no_data} = 3.57; $F_{1,308}$ = 7.167, p < 0.01). Among the covariates age and gender, only age shows a significant influence ($F_{1,308}$ = 10.944, p < 0.01). These results support Hypothesis 1—that is, advertising the storage of movement data providing access for future usage increases consumers' purchase intentions of the smart wearable compared to not saving movement data.

Hypotheses 2. To test Hypotheses 2a–c, three ANCOVAs were performed. The first ANCOVA indicated that participants from Scenario B have higher purchase intentions than participants from Scenario A ($M_{data\_storage}$ = 4.00, M_{no_data} = 3.55; $F_{1,213}$ = 3.892, p < 0.05). Among the covariates age and gender, only age shows a significant influence ($F_{1,213}$ = 9.029, p < 0.01). These results support Hypothesis 2a—that is, advertising the storage of movement data providing access for general future usage (Scenario B) increases consumers' purchase intentions of the smart wearable compared to not saving movement data (Scenario A). Next, the second ANCOVA revealed that purchase intentions increase in Scenario C in comparison with Scenario A (M_{legal_usage} = 4.16, M_{no_data} = 3.56; $F_{1,208}$ = 6.274, p < 0.05). Among the covariates age and gender, again, only age shows a significant influence ($F_{1,208}$ = 5.390, p < 0.05). Hence, these results support Hypothesis 2b—that is, advertising the storage of movement data providing access for future usage to serve as alibi or exculpatory evidence in legal proceedings (Scenario C) increases consumers' purchase intentions of the smart wearable compared to not saving movement data (Scenario A). Finally, the third ANCOVA indicated that purchase intentions did not significantly increase in Scenario C (M_{legal_usage} = 4.18, $M_{data\_storage}$ = 4.05; $F_{1,191}$ = 0.299, p = 0.585) compared to Scenario B. Among the covariates age and gender, only age shows a significant influence ($F_{1,191}$ = 6.966, p < 0.01). Thus, these results do not support Hypothesis 2c—that is, advertising the storage of movement data providing access for the user for future usage to serve as an alibi or exculpatory evidence in legal proceedings (Scenario C) does not increase consumers' purchase intentions of the smart wearable compared to advertising only the storage of movement data providing access for general future usage (Scenario B).

Hypotheses 3. To determine whether data privacy concerns and perceived confidence in court hearings mediate the effect of data usage conditions on purchase intention, we conducted a parallel mediation analysis using Hayes' PROCESS macro (Version 4.0; Model 4, 10,000 bootstrap samples). When comparing Scenario B with Scenario A, results indicate that privacy concerns do not mediate the effect of the possible usage of movement data on consumers' purchase intentions (B = 0.057, SE = 0.056; 95% confidence interval [-0.047; 0.178], not significant (ns)), while there is a significant effect of confidence in court hearings as a mediator (B = 0.204, SE = 0.095; 95% confidence interval [0.026; 0.398], p < 0.01). It is an indirect-only mediation (according to Zhao et al. 2010), as the direct effect of disclosing the possible usage of movement data disappeared in the presence of the mediator (B = 0.191, SE = 0.213; 95% confidence interval [-0.229; 0.612], ns). When comparing Scenario C with Scenario A, our results show that privacy concerns

do not mediate the effect of the possible usage of movement data on consumers' purchase intentions (B = -0.010, SE = 0.031; 95% confidence interval [-0.073; 0.053], ns), while there is a significant effect of confidence in court hearings as a mediator (B = 0.214, SE = 0.063; 95% confidence interval [0.099; 0.346], $p < 0.001$). Again, it is an indirect-only mediation, as the direct effect of disclosing the possible usage of movement data disappeared in the presence of the mediator (B = 0.096, SE = 0.108; 95% confidence interval [-0.117; 0.309], ns). Hence, data privacy concerns do not have a mediating effect, implying that there is no support for Hypothesis 3a. However, confidence in court hearings plays a significant role as a mediator, supporting Hypothesis 3b. As there is no significant difference between Scenario C and Scenario B regarding purchase intention, this also holds true when including both mediators.

4. Experimental Study 2

4.1 Hypothesis Development

In Study 2, we replicated the first study with a different smart wearable—that is, a smart dog collar. The smart dog collar is comparable to the smart wristband in terms of functionality and price range. As a smart wearable it is less familiar for most study participants than the smart wristband, so they cannot rely on previous positive or negative experiences. The main difference for the purpose of our research lies in the fact that the smart dog collar is not worn directly by customers but by their dogs. Although, from a legal point of view, it would always be the human (i.e., the dog owner) being charged in a criminal case (as a dog cannot serve as a defendant in court), the consequences resulting from a legal proceeding can also affect the dog (for instance, when a dog is classified as dangerous and has to be euthanized). Therefore, the perception of dog owners regarding who will suffer possible consequences from legal proceedings is probably different between a smart wristband and a smart dog collar. With respect to the economic relevance of supplies for dogs, it is noteworthy that they constitute a substantial market, given that only in Germany, over 12 million citizens live with at least one dog (Statista 2022b), and revenues for pet supplies (i.e., not just for dogs) in Germany piled up to more than EUR 5.1 billion in 2022 (Statista 2023).

In our first study, we did not find support for Hypothesis 2c. However, we expect this to be different in Study 2 in the context of a smart dog collar because of the special relationship between dog owners and their dogs (Julius et al. 2013). When transferring the child–caregiver attachment theory (Bowlby 1969) to the relationship between dog owners and their dogs, dog owners as caregivers strive to offer comfort in stressful situations ("safe haven effect") and the security to explore the surroundings ("secure base effect"). Hence, dog owners feel responsible for the overall well-being of their dogs. This should also hold true when it comes to legally relevant incidents, as humans can defend themselves against a criminal charge, but dogs cannot explain their actions. Given that the dog depends on the dog owner in its daily life and basic needs (Savalli and Mariti 2020), the dog owner might have special requirements regarding the tracking device. For example, if the dog runs away from home (wearing its smart dog collar) and is subsequently suspected of having attacked an animal or person while not being supervised by the dog owner, this could result in an order to put the dog down. The hope of the dog owners to be able to present warrantable evidence that their dog was, in fact, not at the location of the assault

might therefore have an effect on how the possible advantage in legal proceedings is perceived. Consequently, we expect that dog owners from Scenario C should have a high interest in the storage of movement data that can serve as alibi or exculpatory evidence in legal proceedings if their dogs are involved.

4.2 Study Design

Procedure. The procedure in this second study was essentially the same as in the previous experiment. Participants were asked to put themselves in a situation of looking for a smart dog collar, and participants from all groups were shown the same smart dog collar but received slightly different information about it. While the group of participants from Scenario A was informed that the collected movement data is not saved and hence no one has access to this data afterwards, the second group from Scenario B was informed that the collected movement data is saved locally in the app, and hence, the users have access to this data for future usage if needed. The third group from Scenario C was told that the collected movement data is saved locally in the app, and hence, the users have access to this data for future usage if needed, especially in case of suspicion of a criminal act, when movement data can serve as an alibi or exculpatory evidence in legal proceedings. As in the previous study, all three scenarios were fictitious, and again, we referred to a nonexistent provider called "YouTrack".

Before answering the questionnaire, the participants read the product description and were presented with an advertisement containing the manipulation (see Fig. 2). The items in the questionnaire referred to the dependent variable (i.e., purchase intention), the mediators (i.e., data privacy concerns and confidence in court hearings), the manipulation as well as realism checks, and personal information.

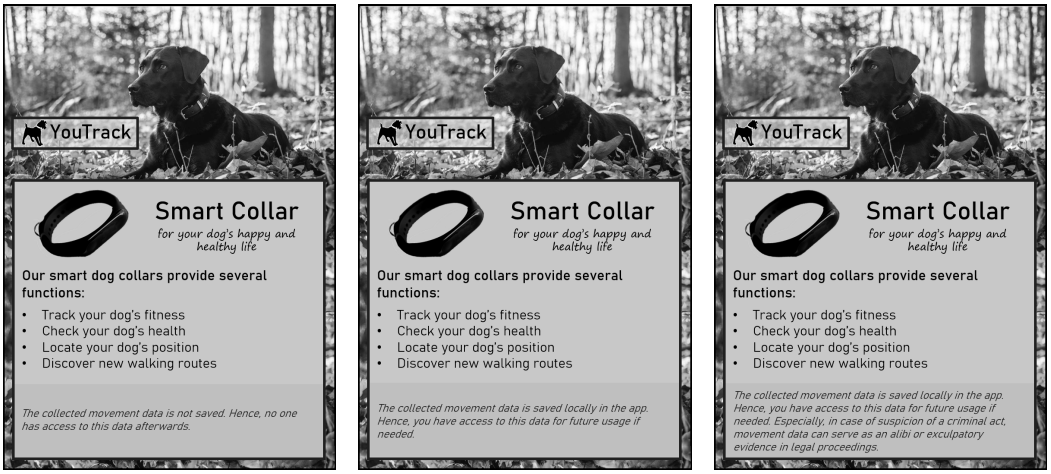


Figure 2: Advertisements Used in Study 2

Sample. Participants were recruited at the end of February 2023 from the same panel that was used in the first study, and thus, the panel provider could exclude participants who had already participated earlier. All 310 participants (49.4% female; M_{age} = 44.5; SD = 14.5) were dog owners from Germany.

Measures. Analogous to the previous study, all items were measured on a 7-point scale from 1 ("strongly disagree") to 7 ("strongly agree"). For purchase intention, we used the scale from the first study (α = 0.952; AVE = 0.786; CR = 0.917). As a matter of course, we also measured for the two mediators—that is, data privacy concerns (α = 0.942; AVE = 0.881; CR = 0.957) and confidence in court hearings (α = 0.949; AVE = 0.781; CR = 0.934)—and we obtained information on gender and age.

4.3 Results

Manipulation and realism checks. We used the same three manipulation checks as in the first study, and they were all successful: results for the first check ("*The scenario description said that the collected movement data are not saved. Hence, no one has access to this data afterwards.*") were M_{no_data} = 4.95, $M_{data\_storage/legal\_usage}$ = 3.43 ($F_{1,308}$ = 41.768, p < 0.001); results for the second check ("*The scenario description said that the collected movement data is saved locally in the app. Hence, you have access to this data for future usage if needed.*") were $M_{data\_storage/legal\_usage}$ = 5.53, M_{no_data} = 4.15 ($F_{1,308}$ = 46.009, p < 0.001); and results for the third check ("*The scenario description said that the collected movement data is saved locally in the app. Hence, you have access to this data for future usage, if needed. Especially, in case of suspicion of a criminal act, movement data can serve as alibi or exculpatory evidence in legal proceedings.*") were $F_{2,307}$ = 28.482, p < 0.001, with planned contrasts at M_{legal_usage} = 5.57, M_{no_data} = 3.76 ($F_{1,307}$ = 49.776, p < 0.001) and M_{legal_usage} = 5.57, $M_{data\_storage}$ = 4.02 ($F_{1,307}$ = 35.977, p < 0.001). The responses to the question of whether the situation was perceived as realistic were also satisfactory (M = 5.20; SD = 1.30).

Hypothesis 1. An ANCOVA indicated that participants from Scenarios B and C did not have significantly higher purchase intentions than participants from Scenario A ($M_{data\_storage/legal\_usage}$ = 4.44, M_{no_data} = 4.14; $F_{1,306}$ = 2.387, p = 0.123). Among the covariates age and gender, only age shows a significant influence ($F_{1,306}$ = 19.144, p < 0.001). These results do not support Hypothesis 1. Hence, advertising the storage of movement data providing access for future usage does not significantly increase consumers' purchase intentions of the smart wearable compared to not saving movement data.

Hypotheses 2. Again, three ANCOVAs were performed to test Hypotheses 2a–c. The first ANCOVA revealed that participants from Scenario B did not have significantly higher purchase intentions than participants from Scenario A ($M_{data\_storage}$ = 4.03, M_{no_data} = 4.11; $F_{1,210}$ = 0.131, p = 0.718). Among the covariates age and gender, only age shows a significant influence ($F_{1,210}$ = 13.132, p < 0.001). These results do not support Hypothesis 2a as advertising the storage of movement data providing access for general future usage (Scenario B) does not significantly increase consumers' purchase intentions of the smart wearable compared to not saving movement data (Scenario A). The second ANCOVA indicated that purchase intentions increase in Scenario C in comparison with Scenario A (M_{legal_usage} = 4.88, M_{no_data} = 4.14; $F_{1,201}$ = 10.588, p < 0.01). Among the covariates age and gender, only age shows a significant influence ($F_{1,201}$ = 10.508, p < 0.01). Thus, these results support Hypothesis 2b—that is, advertising the storage of movement data providing access for future usage to serve as alibi or exculpatory evidence in legal proceedings (Scenario C) increases consumers' purchase intentions of the smart wearable compared to not saving movement data (Scenario A). The third ANCOVA revealed that purchase intentions significantly increased in Scenario C (M_{legal_usage} = 4.87,

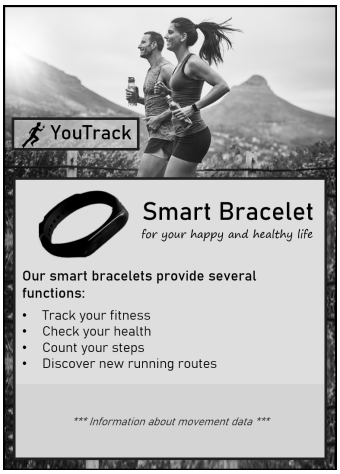
$M_{data\_storage}$ = 4.07; $F_{1,197}$ = 13.639, p < 0.001) compared to Scenario B. Among the covariates age and gender, only age shows a significant influence ($F_{1,197}$ = 10.546, p < 0.01). Thus, these results support Hypothesis 2c—that is, advertising the storage of movement data providing access for the user for future usage to serve as an alibi or exculpatory evidence in legal proceedings (Scenario C) increases consumers' purchase intentions of the smart wearable compared to advertising only the storage of movement data providing access for generic future usage (Scenario B).

Hypotheses 3. In line with Study 1, we conducted a parallel mediation analysis using Hayes' PROCESS macro (Version 4.0; Model 4, 10,000 bootstrap samples) to determine whether data privacy concerns and perceived confidence in court hearings mediate the effect of the data usage condition on purchase intention. First, when comparing Scenario B with Scenario A, results indicate that privacy concerns significantly mediate the effect of the possible usage of movement data on consumers' purchase intentions (B = -0.125, SE = 0.061; 95% confidence interval [-0.258; -0.023], p < 0.01), while there is no significant effect of confidence in court hearings as a mediator (B = 0.040, SE = 0.112; 95% confidence interval [-0.175; 0.261], ns). It was an indirect-only mediation, but the direct effect was neither without nor in the presence of the mediator significant (B = 0.001, SE = 0.202; 95% confidence interval [-0.398; 0.399], ns). Second, when comparing Scenario C with Scenario A, our results show that privacy concerns do not mediate the effect of the possible usage of movement data on purchase intentions (B = -0.021, SE = 0.018; 95% confidence interval [-0.061; 0.009], ns), whereas there is a significant effect of confidence in court hearings as a mediator (B = 0.279, SE = 0.071; 95% confidence interval [0.151; 0.428], p < 0.001). The direct effect of disclosing the possible usage of movement data disappeared in the presence of the mediator (B = 0.113, SE = 0.104; 95% confidence interval [-0.092; 0.318], ns), which also indicates an indirect-only mediation. Third, when comparing Scenario C with Scenario B, our results indicate that privacy concerns do not mediate the effect of the possible usage of movement data on purchase intentions (B = 0.028, SE = 0.039; 95% confidence interval [-0.036; 0.120], ns), while the mediator confidence in court hearings is significant (B = 0.361, SE = 0.117; 95% confidence interval [0.158; 0.617], p < 0.001). The direct effect of disclosing the possible usage of movement data disappeared in the presence of the mediator (B = 0.407, SE = 0.201; 95% confidence interval [-0.011; 0.803], ns). Accordingly, again, it is an indirect-only mediation. Hence, data privacy concerns seem to have a mediating effect when data are stored and can be accessed for general purposes. However, this does not hold true when data are stored in order to serve as alibi or exculpatory evidence in legal proceedings because in the latter case, confidence in court hearings outweighs data privacy concerns. These results imply that there is only partial support for Hypothesis 3a and Hypothesis 3b.

5. Discussion

This work has raised the question of whether the option of being able to use movement data collected and stored by a smart wearable as a prospective benefit in the rare event of being needed in possible legal proceedings can outweigh the wearers' privacy concerns. The answer was not obvious, as prior research suggests that privacy concerns—that is, the secondary use of personal information and perceived intrusion—may constitute a barrier to the adoption of smart consumer products that is not easy to overcome, particularly in a country like Germany, where customers have strong opinions regarding their privacy;

furthermore, prior studies have investigated smart wearables that provide their benefits on a regular basis, which differs from the silent witness functionality in our setting. In order to scrutinize this question, we performed experimental studies featuring two wearables, both of which can be used as silent witnesses. An overview of our findings regarding purchase intention (as hypothesized in H1 and H2) is provided in Table 1.

Smart product:		Smart bracelet	Smart collar
			
Wearer:		Human being	Dog
H1:	B + C > A	✓	✗
H2a:	B > A	✓	✗
H2b:	C > A	✓	✓
H2c:	C > B	✗	✓

The letters A, B, and C refer to the three scenarios used in the experimental studies:
A: "The collected movement data is not saved. Hence, no one has access to this data afterwards."
B: "The collected movement data are saved locally in the app. Hence, you have access to this data for future usage if needed."
C: "The collected movement data are saved locally in the app. Hence, you have access to this data for future usage, if needed. Especially, in case of suspicion of a criminal act, movement data can serve as alibi or exculpatory evidence in legal proceedings."

Table 1: Overview of design und results from the two experimental studies

It turns out that purchase intentions are higher for a smart wearable that collects movement data for general purposes and can also serve as a silent witness (i.e., a smart wearable from Scenario C) than for a smart wearable that does not save any movement data (i.e., a smart wearable from Scenario A). This finding holds true for both wearables. However, and most interestingly, we found a difference with respect to the (perceived) beneficiary of the storage of movement data for general purposes and the silent witness service, respectively:

For the smart wristband, our results indicate that purchase intentions are higher in Scenario B than in Scenario A, which suggests that consumers appreciate the availability of movement data for general purposes (e.g., as a means of monitoring their fitness training).

This finding fits with earlier research (e.g., Kuru 2016). Beyond this benefit, the additional silent witness functionality does not seem to provide a substantial extra value (as there is no significant difference regarding purchase intentions between Scenarios B and C).

In contrast, for the smart dog collar, the participants did not express a higher willingness to purchase the dog collar just because the dog's movement data are saved (i.e., there is no significant difference in purchase intentions between Scenarios A and B). A reason may be that consumers do not perceive the value added from the dog's movement data as particularly high (as, probably, they do not have in mind a specific use case for these data). Instead, participants seem to appreciate the alibi functionality of the smart dog collar, as their willingness to purchase the smart dog collar is higher in Scenario C than in Scenario B. This mindset is in line with child–caregiver attachment theory (Bowlby 1969), according to which, by analogy, dog owners care about their dogs and want to protect them also in the (rare) event of the dogs being involved in some legal proceedings. As the smart dog collar in Scenario C collects movement data that can be used as alibi or exculpatory evidence in such possible legal proceedings, our results suggest that this function provides a sufficiently high value added.

Regarding privacy concerns as a mediator (as hypothesized in H3a), the results of our studies indicate that they do not play a role, with the only exception when comparing Scenarios A and B for the dog collar (for which, however, no main effect was detected). This finding is surprising, as in most related studies, privacy concerns are an important factor. A possible explanation is that we described the data as being saved locally (and not in the cloud or at the site of the service provider), which might have diminished privacy concerns by the participants. Regarding confidence in court hearings as a mediator (as hypothesized in H3b), we find the expected positive effect in all instances for which we identified significant main effects.

The managerial implications of these findings are not limited to providers of smart wearables, who might opt to advertise the above-mentioned advantage, but are also valid for producers of certain other smart products that can store sensitive data for various purposes (e.g., smartphones or dashcams in cars). Our results hint that consumers' sensibility regarding privacy concerns when smart products collect and store movement data might be overrated to some extent, and seems to disappear if smart products use such data for offering sufficiently beneficial services to their customers. However, the value added might stem from consumers' affective needs. Our study shows that this is not the case for the smart bracelet (once the movement data are stored for general purposes) but for the smart dog collar. If so, it seems to be fine that the respective benefit is only realized in rare events (or even never).

6. Limitations and Further Research

Our study features an innovative application case, which entails several limitations but also offers opportunities for further research. First, we portrayed the silent witness functionality primarily as helpful. However, not all people would subscribe to the underlying idea that "if you've got nothing to hide, you've nothing to worry about," but they may perceive the collection of movement data as a risk. Therefore, consumers' notions of the silent witness with respect to both benefits and risks should be investigated in more depth.

Second, the owner of the smart wearable might ask somebody else to wear the silent witness at a certain time, which obviously limits the value of the collected movement data

as exculpatory evidence. Probably, a (technical) solution for this issue will be available in the future, but until then, the value of the witness functionality is criticizable.

Third, we framed the description of the possible benefit from the smart wearables carrying the silent witness functionality to incidents related to criminal law. As an extension, it would be interesting to see whether the effect would be the same if participants in a subsequent study were told that movement data are used for general law compliance monitoring—for example, to prosecute traffic offenses like speeding.

Fourth, we informed the participants in our studies that the sensible movement data were saved locally, which might have attenuated privacy concerns. Another study could inform them that their movement data are stored in a data cloud or at the service provider's site, which might result in more substantial data privacy concerns.

Fifth, we collected data only from Germany. Therefore, it would be interesting to replicate the study in other countries, particularly in countries where privacy concerns regarding smart products are less pronounced (e.g., Sweden, China, or South Korea; Statista 2022a).

Sixth, it could be worthwhile to study additional mediators (other than privacy concerns and confidence in court hearings) that may play a relevant role in the adoption of smart products. Trust appears to be a prime candidate for this purpose. In such a future study, certain trust-building factors—such as security and protection, brand, or product performance (Michler et al. 2020)—may be manipulated to investigate whether privacy concerns would also be outweighed in these cases.

Seventh, our research is limited to the storage of movement data that are mostly collected outdoors by a smart wearable. Hence, an extension from movement data to voice data (e.g., the usage of voice data from smart speakers) and corresponding, possibly different, effects could be studied in the future.

Overall, ambient intelligent environments, in which electronic devices constantly monitor human behavior, can raise new forms of consumer concern. More research is required to learn about these concerns and to discuss the corresponding managerial implications.

References

Altimari, D. (2018): All Evidence Turned over as Fitbit Murder Case Moves Toward Trial, in: Hartford Courant, July 20, 2018. http://www.courant.com/news/connecticut/hc-news-fit-bit-murder-dabate-trial-20180720-story.html [http://perma.cc/GE5B-V3GG], retrieved May 27, 2023.

Armstrong, J. S./Brodie, R. J./Parsons, A. G. (2001): Hypotheses in Marketing Science: Literature Review and Publication Audit, in: Marketing Letters, Vol. 12, No. 2, pp. 171–187.

Bayoumy, K./Gaber, M./Elshafeey, A./Mhaimeed, O./Dineen, E. H./Marvel, F. A./Martin, S. S./Muse, E. D./Turakhia, M. P./Tarakji, K. G./Elshazly, M. B. (2021): Smart Wearable Devices in Cardiovascular Care: Where We Are and How to Move Forward, in: Nature Reviews Cardiology, Vol. 18, No. 8, pp. 581–599.

Becker, M./Matt, C./Widjaja, T./Hess, T. (2017): Understanding Privacy Risk Perceptions of Consumer Health Wearables: An Empirical Taxonomy, in: Proceedings of the International Conference on Information Systems (ICIS) 2017, Paper 12.

Bleier, A./Eisenbeiss, M. (2015): The Importance of Trust for Personalized Online Advertising, in: Journal of Retailing, Vol. 91, No. 3, pp. 390–409.

Bowlby, J. (1969): Attachment and Loss. Basic Books.

Briquelet, K. (2017): My Fitbit Proves I Didn't Kill Her, in: The Daily Beast, June 06, 2017. http://www.thedailybeast.com/my-fitbit-proves-i-didnt-kill-her [http://perma.cc/AJ9D-R456], retrieved May 27, 2023.

Clarke, R. (1999): Internet Privacy Concerns Confirm the Case for Intervention, in: Communications of the ACM, Vol. 42, No. 2, pp. 60–67.

Culnan, M. J./Armstrong, P. K. (1999): Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation, in: Organization Science, Vol. 10, No. 1, pp. 104–115.

Darke, P./Brady, M. K./Benedicktus, R. L./Wilson, A. E. (2016): Feeling Close From Afar: The Role of Psychological Distance in Offsetting Distrust in Unfamiliar Online Retailers, in: Journal of Retailing, Vol. 92, No. 3, pp. 287–299.

Dawid, H./Decker, R./Hermann, T./Jahnke, H./Klat, W./König, R./Stummer, C. (2017): Management Science in the Era of Smart Consumer Products: Challenges and Research Perspectives, in: Central European Journal of Operations Research, Vol. 25, No. 1, pp. 203–230.

Decker, R./Stummer, C. (2017): Marketing Management for Consumer Products in the Era of the Internet of Things, in: Advances in Internet of Things, Vol. 7, No. 3, pp. 47–70.

El-Gayar, O./Elnoshokaty, A./Behrens, A. (2021): Understanding Design Features for Continued Use of Wearables Devices, in: Proceedings of the Americas Conference on Information Systems (AMCIS), Paper 1353.

Fährmann, J. (2020): Digitale Beweismittel und Datenmengen im Strafprozess, in: Multimedia und Recht, Vol. 23, No. 4, pp. 228–238.

Fuchs, C./Schreier, M./ Van Osselaer, S. M. J. (2015): The Handmade Effect: What's Love Got to Do with It?, in: Journal of Marketing, Vol. 79, No. 2, pp. 98–110.

Gao, Y./Li, H./Luo, Y. (2015): An Empirical Study of Wearable Technology Acceptance in Healthcare, in: Industrial Management & Data Systems, Vol. 115, No. 9, pp. 1704–1723.

Gless, S./Stagno, D. (2018): Digitale Assistenten und strafprozessuale Beweisführung, in: Schweizerische Juristen-Zeitung, Vol. 114, No. 12, pp. 289–297.

GlobeNewswire (2023): Smart Wearable Market Growth Accelerating at a CAGR of 15.3% with Rise in Ongoing Trend of Tech-Savvy Customers. https://www.globenewswire.com/en/news-release/2023/04/13/2646319/0/en/Smart-Wearable-Market-Growth-Accelerating-at-a-CAGR-of-15-3-With-Rise-in-Ongoing-Trend-of-Tech-Savvy-Customers.html, retrieved May 10, 2023.

Hanelt, A./Bohnsack, R./Marz, D./Marante, C. A. (2021): A Systematic Review of the Literature on Digital Transformation: Insights and Implications for Strategy and Organizational Change, in: Journal of Management Studies, Vol. 58, No. 5, pp. 1159–1197.

Hauser, C. (2017): In Connecticut Murder Case, a Fitbit is a Silent Witness, in: New York Times, April 27, 2017. https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html, retrieved April 12, 2023.

Hauser, C. (2018): Police use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing, in: New York Times, October 3, 2018. https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html, retrieved April 12, 2023.

Hayes, A. F. (2018): Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach, 2nd ed., Guildford Press.

Jabbar, A./Geebren, A./Hussain, Z./Dani, S./Ul-Durar, S. (2023): Investigating Individual Privacy within CBDC: A Privacy Calculus Perspective, in: Research in International Business and Finance, Vol. 64, Paper 101826.

Julius, H./Beetz, A./Kotrschal, K./Turner, D. C./Uvnäs-Moberg, K. (2013): Attachment to Pets, Hogrefe.

Kaiser, I./Stummer, C. (2020): How the Traditional Industrial Manufacturer Miele Established a New Smart Home Division, in: Research-Technology Management, Vol. 63, No. 4, pp. 29–34.

Kehr, F./Kowatsch, T./Wentzel, D./Fleisch, E. (2015): Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus, in: Information Systems Journal, Vol. 25, No. 6, pp. 607–635.

Kendall, W. (2019): "Outrunning" the Fourth Amendment: A Functional Approach to Searches of Wearable Fitness Tracking Devices, in: Southern Illinois University Law Journal, Vol. 43, pp. 333–360.

Kim, D./Park, K./ Park, Y./Ahn, J.-H. (2019): Willingness to Provide Personal Information: Perspective of Privacy Calculus in IoT Services, in: Computers in Human Behavior, Vol. 92, pp. 273–281.

Kuru, A. (2016): Exploring Experience of Runners with Sports Tracking Technology, in: International Journal of Human–Computer Interaction, Vol. 32, No. 11, pp. 847–860.

Langley, D. J./van Doorn, J./Ng, I. C. L./ Stieglitz, S./Lazovik, A./Boonstra, A. (2021): The Internet of Everything: Smart Things and Their Impact on Business Models, in: Journal of Business Research, Vol. 122, pp. 853–863.

Laufer, R. S./Wolfe, M. (1977): Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory, in: Journal of Social Issues, Vol. 33, No. 3, pp. 22–42.

Li, H./Wu, J./Gao, Y./Shi, Y. (2016): Examining Individuals' Adoption of Healthcare Wearable Devices: An Empirical Study from Privacy Calculus Perspective, in: International Journal of Medical Informatics, Vol. 88, pp. 8–17.

Luo, X. (2002): Trust Production and Privacy Concerns on the Internet: A Framework Based on Relationship Marketing and Social Exchange Theory, in: Industrial Marketing Management, Vol. 31, No. 2, pp. 111–118.

Mani, Z./Chouk, I. (2019): Impact of Privacy Concerns on Resistance to Smart Services: Does the 'Big Brother Effect' Matter?, in: Journal of Marketing Management, Vol. 35, No. 15–16, pp. 1460–1479.

Maxham, J. G./Netemeyer, R. G. (2002): A Longitudinal Study of Complaining Customers' Evaluations of Multiple Service Failures and Recovery Efforts, in: Journal of Marketing, Vol. 66, No. 4, pp. 57–71.

Michler O./Decker, R./Stummer, C. (2020): To Trust or Not to Trust Smart Consumer Products: A Literature Review of Trust-Building Factors, in: Management Review Quarterly, Vol. 70, No. 3, pp. 391–420.

Michler, O./Stummer, C./Decker, R. (2022): Can the GDPR Allay Privacy Concerns Towards Smart Products? The Effect of a Compliance Seal on Perceived Data Security, Trust, and Intention to Use, in: Kö, A./Francesconi, E./Kotsis, G./Tjoa, A. M./Khalil, I. (Eds), Proceedings of the International Conference on Electronic Government and the Information Systems Perspective (EGOVIS), Lecture Notes in Computer Science 13429, Springer, pp. 77–91.

Morgan, R./Hunt, S. D. (1994): The Commitment–Trust Theory of Relationship Marketing, in: Journal of Marketing, Vol. 58, No. 3, pp. 20–38.

Naous, D./Kulkarni, V./Legner, C./Garbinato, B. (2019): Information Disclosure in Location-Based Services: An Extended Privacy Calculus Model, in: Proceedings of the International Conference on Information Systems (ICIS), Paper 40.

Nahavandi, D./Alizadehsani, R./Khosravi, A./Acharya, U. R. (2022): Application of Artificial Intelligence in Wearable Devices: Opportunities and Challenges, in: Computer Methods and Programs in Biomedicice, Vol. 213, Paper 106541.

Nascimento, B./Oliveira, T./Tam, C. (2018): Wearable Technology: What Explains Continuance Intention in Smartwatches?, in: Journal of Retailing and Consumer Services, Vol. 43, pp. 157–169.

Oh, J./Kang, H. (2021): User Engagement with Smart Wearables: Four Defining Factors and a Process Model, in: Mobile Media & Communication, Vol. 9, No. 2, pp. 314–335.

Paul, C. (2020): Privacy Concerns Regarding Wearable IoT Devices: How It is Influenced by GDPR?, in: Proceedings of Hawaii International Conference on Systems Sciences (HICSS-53), pp. 4388–4397.

Podsakoff, P. M./Podsakoff, N. P. (2019): Experimental Designs in Management and Leadership Research: Strengths, Limitations, and Recommendations for Improving Publishability, in: Leadership Quarterly, Vol. 30, No. 1, pp. 11–33.

Porter, M. E./Heppelmann, J. E. (2014): How Smart, Connected Products are Transforming Competition, in: Harvard Business Review, Vol. 92, No. 11, pp. 64–88.

Porter, M. E./Heppelmann, J. E. (2015): How Smart, Connected Products are Transforming Companies, in: Harvard Business Review, Vol. 93, No. 10, pp. 96–114.

Poythress, N. G./Petrila, J./McGaha, A./Boothroyd, R. (2002): Perceived Coercion and Procedural Justice in the Broward Mental Health Court, in: International Journal of Law and Psychiatry, Vol. 25, No. 5, pp. 517–533.

Princi, E./Krämer, N. (2020): I Spy With My Little Sensor Eye: Effect of Data-Tracking and Convenience on the Intention to Use Smart Technology, in: Proceedings of Hawaii International Conference on Systems Sciences (HICSS-53), pp. 1391–1400.

Psychoula, I./Chen, L./Amft, O. (2020): Privacy Risk Awareness in Wearables and the Internet of Things, in: IEEE Pervasive Computing, Vol. 19, No. 3, pp. 60–66.

Raff, S./Wentzel, D./Obwegeser, N. (2020): Smart Products: Conceptual Review, Synthesis, and Research Directions, in: Journal of Product Innovation Management, Vol. 37, No. 5, pp. 379–404.

Reichheld, F./Schefter, P. (2000): E-Loyalty: Your Secret Weapon on the Web, in: Harvard Business Review, Vol. 78, No. 4, pp. 105–113.

Rodis, A. (2020): Fitbit Data and the Fourth Amendment: Why the Collection of Data from a Fitbit Constitutes a Search and Should Require a Warrant in Light of Carpenter v. United States, in: William & Mary Bill of Rights Journal, Vol., 29, No. 2, pp. 533–559.

Savalli, C./Mariti, C. (2020): Would the Dog be a Person's Child or Best Friend? Revisiting the Dog-Tutor Attachment, in: Frontiers in Psychology, Vol. 11, Article 576713.

Schleef M., Rademacher T., Stummer C. (2022): The Spy Who Saves Me: Can Emergency Detection Capabilities in a Smart Home Environment Outweigh Data Usage Concerns?, in: Proceedings of the Pacific Asia Conference on Information Systems (PACIS), Paper 114.

Schmidt, J./Bijmolt, T. H. A. (2020): Accurately Measuring Willingness to Pay for Consumer Goods: A Meta-Analysis of the Hypothetical Bias, in: Journal of the Academy of Marketing Science, Vol. 48, No. 3, pp. 499–518.

Schomakers, E.-M./Lidynia, C./Ziefle, M. (2022): The Role of Privacy in the Acceptance of Smart Technologies: Applying the Privacy Calculus to Technology Acceptance, in: International Journal of Human–Computer Interaction, Vol. 38, No. 13, pp. 1276–1289.

Shaw, N./Sergueeva, K. (2016): Convenient or Useful? Consumer Adoption of Smartphones for Mobile Commerce, in: Diffusion Interest Group in Information Technology (DIGIT) Proceedings, Paper 3.

Silverman, E./Arnold, J./Gless, S. (2024): Robot Testimony? A Taxonomy and Standardized Approach to Evaluative Data in Criminal Proceedings, in: Gless, S./Whalen-Bridge, H. (Eds), Human–Robot Interaction in Law and Its Narratives: Legal Blame, Procedure, and Criminal Law, Cambridge University Press, pp. 167–191.

Statista (2015): Anteil an Personen mit Datenschutz-Bedenken in ausgewählten Ländern Europas im Jahr 2015, https://de.statista.com/statistik/daten/studie/415956/umfrage/bedenken-beim-datenschutz-in-europa-nach-laendern/, retrieved April 04, 2023.

Statista (2022a): Importance of Smart Home Security & Safety/Worried about Being Spied on Through Smart Home Devices 2021, by Country, https://www.statista.com/forecasts/1227824/smart-home-security-safety-vs-privacy-concerns, retrieved April 12, 2023.

Statista (2022b): Pet Owners in Germany by Number of Dogs in Households from 2018 to 2021, https://de.statista.com/statistik/daten/studie/181167/umfrage/haustier-anzahl-hunde-im-haushalt/, retrieved April 22, 2022.

Statista (2023): Revenue from Physical and Online Store Pet Supply Sales in Germany from 2006 to 2022, https://www.statista.com/statistics/556093/pet-supply-sales-physical-vs-online-stores-germany/, retrieved May 19, 2023.

Steele, R. (2022): Equalizing Access to Evidence: Criminal Defendants and the Stored Communications Act, in: Yale Law Journal, Vol. 131, No. 5, pp. 1385–1718.

Thompson, R./Compeau, D./Higgins, C./Lupton, N. C. (2008): Intentions to Use Information Technologies: An Integrative Model, in: End User Computing Challenges and Technologies: Emerging Tools and Applications, pp. 79–101.

Venkatesh, V./Morris, M. G./Davis, G. B./Davis, F. D. (2003): User Acceptance of Information Technology: Toward a Unified View, in: MIS Quarterly, Vol. 27, No. 3, pp. 425–478.

Wallace, A./Goodman-Delahunty, J. (2021): Measuring Trust and Confidence in Courts, in: International Journal for Court Administration, Vol. 12, No. 3, pp. 1–17.

Zhang, T./Dong, P./Zeng, Y./Ju, Y. (2022): Analyzing the Diffusion of Competitive Smart Wearable Devices: An Agent-Based Multi-Dimensional Relative Agreement Model, in: Journal of Business Research, Vol. 139, No. 4, pp. 90–105.

Zhao, X./Lynch, J. G./Chen, Q. (2010): Reconsidering Baron and Kenny: Myths and Truths about Mediation Analysis, in: Journal of Consumer Research, Vol. 37, No. 2, pp. 197–206.

Melina Schleef, Dr., ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Innovations- und Technologiemanagement an der Universität Bielefeld.

Anschrift: Universität Bielefeld, Lehrstuhl für Innovations- und Technologiemanagement, Universitätsstr. 25, 33615 Bielefeld, Deutschland, Tel.: 0049–521–106–4844, E-Mail: melina.schleef@uni-bielefeld.de

Sabine Gless, Dr., ist Professorin für Strafrecht und Strafprozessrecht an der Universität Basel.

Anschrift: Universität Basel, Lehrstuhl für Strafrecht und Strafprozessrecht, Peter Merian-Weg 8, 4052 Basel, Tel.: 0041–61–207–2873, E-Mail: sabine.gless@unibas.ch

Christian Stummer, Dr., ist Professor für Innovations- und Technologiemanagement sowie Direktor des Instituts für Technologische Innovationen, Marktentwicklung und Entrepreneurship (iTIME) an der Universität Bielefeld.

Anschrift: Universität Bielefeld, Lehrstuhl für Innovations- und Technologiemanagement, Universitätsstr. 25, 33615 Bielefeld, Deutschland, Tel.: 0049–521–106–4892, E-Mail: christian.stummer@uni-bielefeld.de

Acknowledgement: This research was conducted in the course of the ZiF Research Group on "Economic and Legal Challenges in the Advent of Smart Products" (October 2021 – July 2022). We thank the members of the group for their valuable feedback during the early stages of our research endeavor. Financial support from the Center for Interdisciplinary Research (ZiF) is gratefully acknowledged.