Wintmölle, Florian; Meier, Marco; Maier, Christian

Privacy over health? : Understanding discontinuous disclosure in mobile health applications

Date of secondary publication: 12.12.2025

Version of Record (Published Version), Article

Persistent identifier: urn:nbn:de:bvb:473-irb-112136x

Primary publication

Wintmölle, Florian; Meier, Marco; Maier, Christian (2026): Privacy over health? : Understanding discontinuous disclosure in mobile health applications, in: Information & management : the international journal of information systems applications, Amsterdam [u.a.]: Elsevier Science, Vol. 63, Nr. 2, 104277, pp. 1–19, doi: 10.1016/j.im.2025.104277.

Information & Management 63 (2026) 104277

Contents lists available at ScienceDirect

Information & Management

journal homepage: www.elsevier.com/locate/im

Privacy over health? Understanding discontinuous disclosure in mobile health applications

Florian Wintmölle *, Marco Meier, Christian Maier

Information Systems, Health and Society in the Digital Age, University of Bamberg, Gutenbergstraße 13, Bamberg 96050, Germany

ARTICLE INFO

Keywords:
Privacy calculus theory
Discontinuous disclosure
Mobile health applications (mHealth apps)
Two-step Fuzzy Set Qualitative Comparative Analysis (fsQCA)
Misuse

ABSTRACT

Practice shows that many users stop disclosing personal health information (PHI) in mobile health applications due to privacy concerns about potential misuse, thereby foregoing potential health benefits. We draw on privacy calculus theory to explain the reasons for this deliberate behavioral shift, which we label discontinuous disclosure. Privacy calculus theory states that users weigh the benefits of disclosure against the associated costs. We suggest that discontinuous disclosure arises from a discrepancy in users' perceptions regarding these benefits and costs. Initially, they expect benefits from their PHI disclosure (e.g., health benefits) but subsequently do not experience these benefits or encounter unexpected costs (e.g., privacy concerns), which eventually lead them to discontinue disclosing. To account for such changing perceptions over time, we suggest that a combination of initial expectations and subsequent experiences regarding disclosure benefits and costs leads to discontinuous disclosure. We conducted a two-step fuzzy-set qualitative comparative analysis on survey data from 322 mobile health application users and reveal four configurations that explain discontinuous disclosure. We contribute to privacy research by introducing discontinuous disclosure as a novel disclosure behavior characterized by the discrepancy between expectations and experiences. We also extend privacy calculus theory by shifting from a static, one-time tradeoff to a dynamic view where (1) initial expectations form a baseline for assessing subsequent experiences and (2) experienced and expected benefits and costs work together to explain disclosure behavior. Additionally, we contribute to IS research on mobile health applications by explaining users' disclosure behavior in this context.

1. Introduction

Recent public discourse highlights a critical privacy issue: the possibility that personal health information (PHI) from mobile health applications (mHealth apps) could be misused in legal proceedings. A prominent example involves the misuse of PHI from period trackers by authorities in US states with restrictive abortion laws, which has prompted many users to delete these apps to prevent their PHI from being disclosed [1,2]. In fact, this salient example reflects a broader pattern in which users often stop disclosing PHI after some time due to privacy concerns [3]. We refer to this behavior as *discontinuous disclosure*.

While such discontinuous disclosure may protect users' privacy, it also eliminates the potential benefits of using mHealth apps that range from personalized fertility guidance to preventing cardiovascular risks [4,5]. Notably, these benefits are contingent on users' willingness to disclose sensitive PHI, such as menstrual cycle patterns for managing reproductive health and heart rate records for detecting potential irregularities, a practice that inherently raises privacy concerns [3,5]. These privacy concerns are further exacerbated today by artificial intelligence (AI), particularly through potential AI misuse by mHealth apps, as their modern, AI-driven data analysis can deduce sensitive insights (e.g., a pregnancy) from PHI that was never explicitly shared [6]. Ultimately, this results in a dilemma in which users face a tradeoff between substantial potential benefits and serious privacy concerns.

To understand such tradeoffs, research draws on privacy calculus theory, which has been used in various contexts, including e-commerce [7], online social networks [8], and health [9], to explain users' disclosure behavior. It states that users weigh the benefits of disclosure (e.g., health benefits) against the associated costs (e.g., privacy concerns) and disclose their personal information when the benefits outweigh the costs [10]. Prior work builds on privacy calculus theory to explain the reasons users initially disclose personal information [11–14] and the reasons they continue to do so [15]. However, this research falls

* Corresponding author.
E-mail address: florian.wintmoelle@uni-bamberg.de (F. Wintmölle).

https://doi.org/10.1016/j.im.2025.104277
Received 4 December 2024; Received in revised form 18 November 2025; Accepted 23 November 2025
Available online 24 November 2025

short of explaining why users reverse their behavior and discontinue disclosing after initial voluntary disclosure. We use this as an opportunity to position discontinuous disclosure as a conceptually distinct disclosure behavior, requiring a new dynamic explanation that accounts for temporal dissonance in light of the inherent behavioral shift.

Unlike continuous disclosure, which results from alignment between expected and experienced benefits and costs [15], discontinuous disclosure arises from a discrepancy between them. Theoretically, this means that users initially have positive expectations but then experience insufficient benefits or face unexpected costs, such as privacy concerns, whose negative consequences often occur with a delay and only become apparent at a later stage [16]. This discrepancy between initial expectations and subsequent experiences triggers a re-evaluation of the disclosure choice, prompting users to discontinue disclosure if this new tradeoff becomes negative, with experienced costs outweighing the benefits.

To account for this discrepancy, it is theoretically insufficient to model experienced tradeoffs in isolation, as is the case with explanations of known disclosure behaviors [7,14,15]. Instead, we propose a two-step perspective with users' expected benefits and costs forming a baseline upon which they later weigh their experienced benefits and costs. The discrepancy between both stages then explains the reversal in their behavior, leading us to ask the following research question:

How do expected and experienced benefits and costs together lead to users' discontinuous disclosure of PHI?

To answer this question, we employed an inductive approach using two-step fuzzy set qualitative comparative analysis (fsQCA) on survey data from 322 mHealth app users [17]. We identified four combinations, consisting of different expected and experienced benefits and costs, referred to as configurations, that lead to users' discontinuous disclosure of PHI in mHealth apps. Based on these configurations, we develop five propositions that explain the theoretical mechanisms by which expected and experienced benefits and costs together lead to discontinuous disclosure.

We contribute to privacy research by introducing discontinuous disclosure as a novel and theoretically distinct disclosure behavior, marked by a behavioral shift where users deliberately reverse their initial choice to disclose personal information. By developing an explanation for this behavior, we contribute to privacy calculus theory by shifting its focus from a static, one-time tradeoff to a dynamic, two-step perspective. This dynamic view demonstrates that expected and experienced benefits and costs must be considered together, as users' initial expectations form a crucial baseline upon which they later weigh their actual experiences. Finally, we contribute to research on mHealth apps by explaining users' disclosure behavior in this context.

2. Theoretical background

This section establishes the theoretical foundation for our study. We begin by examining the unique context of mHealth apps and the factors that influence users' choice to disclose their PHI. We then introduce privacy calculus theory as a theoretical lens for understanding disclosure behaviors.

2.1. Mobile health applications

2.1.1. Functions of mobile health applications

Mobile health applications (mHealth apps) refer to software solutions for smartphones that aim to improve their users' health by enabling them to better monitor and self-regulate their personal lifestyle choices and health, such as their nutrition, weight loss, daily physical activity, and menstrual cycle [18,19]. By collecting and processing such PHI, mHealth apps can offer users helpful insights into their health [18]. For example, they use the PHI to encourage users to improve their nutrition by providing personalized dietary recommendations to lose weight, increase their daily physical activity by suggesting more steps or setting personalized fitness goals, or indicate potential health issues by identifying irregularities in users' menstrual cycle [20,21]. Devices that collect PHI through biomedical sensors, such as wearables, further expand the capabilities of mHealth apps by incorporating sensory information from a user's body, including their sleep patterns and heart rate [22]. Examples of mHealth apps include MyFitnessPal, which allows users to track their calorie intake when eating and their weight loss progress, and Apple Health, which allows them to monitor their daily physical activity and menstrual cycle.

Thus, while mHealth apps are potentially advantageous for users, their core functionality, such as their capacity to provide health insights, fundamentally depends on users providing their PHI. This information is inherently sensitive because it details a user's physical and mental well-being and, if misused, could lead to consequences ranging from targeted advertising to discrimination [9,23]. This creates a fundamental tension: to benefit from the app, users must disclose precisely the sensitive information that could expose them to risk. Accordingly, understanding this disclosure behavior in mHealth apps is crucial.

2.1.2. Disclosure in mobile health applications

Disclosure describes users' behavior regarding the sharing of personal information with others [13,24]. In the health context, this disclosure focuses on the sharing of PHI [23]. Building on prior research, we next outline the main factors that explain disclosure behavior in the mHealth app context. We provide an overview of these factors in Table 1.

At their core, mHealth apps' primary value proposition lies in their promise of improving users' health, which implies that users expect them to improve their health in some way [18,27]. Health benefits encompass any perceived positive impact on users' physical, mental, or social health that they expect from engaging with the app and disclosing their PHI [9,25,28]. By enabling features such as monitoring, tracking, and self-regulation of personal lifestyle choices [18,27], mHealth apps

Table 1
Factors explaining disclosure behavior in the context of mHealth apps.

	Definition	Example
Health benefits (based on [25])	Describes the extent to which users believe that disclosing their PHI to an mHealth app leads to positive health outcomes	Users may believe that providing PHI about their physical activity and nutrition will lead to better weight management
Personalization (based on [13])	Describes the extent to which users believe that disclosing their PHI to an mHealth app allows the mHealth app to be tailored to their activity contexts, preferences, and needs	Users may believe that by providing PHI about their exercise habits and dietary preferences, an mHealth app can generate customized meal plans and workout schedules
Trust (based on [26])	Describes the extent to which users believe that an mHealth app is dependable in protecting their PHI	Users may believe that an mHealth app has strong encryption and privacy policies in place to keep their PHI secure from unauthorized access
Privacy concerns (based on [7])	Describes the extent to which users are concerned about opportunistic behavior like secondary use by the mHealth app related to their PHI disclosed	Users may be concerned that an mHealth app might sell their PHI to third-party marketers without their consent

foster strong user expectations of tangible health improvements. For instance, users expect that tracking their calorie intake or daily steps will help them lose weight by encouraging a healthy lifestyle [28]. Given this direct link to the mHealth app's core purpose, these expected health benefits represent the primary functional utility that motivates users to disclose their PHI.

The provision of tailored services (i.e., personalization) is widely recognized as a key driver of user value across various digital contexts [13,14]. It is rooted in the personalization-privacy paradox, where users willingly provide personal information in exchange for more relevant services and content [29]. As a direct benefit, personalization provides utility by proactively tailoring services to a user's needs and context [14, 30], which reduces information overload and cognitive effort for the user [31,32], creating a more efficient and gratifying user experience [32]. This utility is particularly vital in the mHealth context. Here, health and lifestyle choices, such as diet, smoking, or physical activity, are inherently individual [33], making personalization a crucial factor for engagement [34,35]. More specifically, users expect mHealth apps to provide context-aware service delivery explicitly tailored to their individual needs [36,37], often leveraging usage and activity data from smartphones and sensors for individualized insights [38] (e.g., steps taken). This focus on the quality and relevance of the mHealth app's service delivery positions personalization as a distinct functional utility of the app that users value independently of specific health benefits. Consequently, the expectation of receiving such personalization is crucial for users' willingness to disclose their PHI.

mHealth apps leverage highly sensitive PHI, making users' trust in the appropriate handling of this information essential [23]. Conceptually, trust describes the belief that the mHealth app is dependable in protecting a user's personal information [26] and will not use it opportunistically [7]. It is often regarded as a confidence belief, an expectation of users that their personal information will be handled competently, reliably, and safely, thereby reducing the uncertainty and perceived risks inherent in online environments [7]. Although distinct from direct functional utilities like health benefits and personalization, trust's primary function is to serve as a crucial enabling factor for disclosure [23]. Specifically, it empowers users to disclose the PHI necessary to unlock the mHealth app's functional utilities in the first place. This enabling effect operates through the psychological mechanism in which trust mitigates the inherent anxiety associated with disclosing sensitive personal information, thereby fostering a sense of peace of mind and emotional security for the user [7,23]. This function is particularly important in the health context because there is naturally an information asymmetry that leads to uncertainty that trust helps to overcome [23,39]. Given its focus on creating a safe interaction environment rather than delivering a direct service output, trust therefore serves as a crucial enabling factor for users' willingness to disclose their PHI despite underlying concerns [23].

Users who disclose personal information face the threat that this information may be misused or lost due to opportunistic behavior by an organization [40,41]. Privacy concerns represent an internalization of this potential loss and describe users' assessment of what might happen to the information disclosed [7], making them inherently hesitant to disclose. In the health context, privacy concerns are particularly pronounced due to the high sensitivity of PHI [23], which can evoke strong negative reactions and increase fears of potential negative outcomes. Therefore, privacy concerns constitute a crucial factor that hinders users' willingness to disclose their PHI as they actively seek to avoid putting their data at risk.

In sum, these factors constitute distinct but complementary facets of a user's decision to disclose PHI. Users are essentially motivated to disclose by positive drivers – the functional utilities of health benefits and personalization, which are enabled by trust. These drivers are directly counteracted by privacy concerns, which represent the potential for adverse consequences of such disclosure. This distinction between positive drivers and adverse consequences in explaining disclosure behavior resonates well with privacy calculus theory, to which we therefore turn next.

2.2. Privacy calculus theory

Privacy calculus theory suggests that users weigh the benefits of disclosing personal information against the associated costs of doing so [42]. More specifically, users disclose their personal information when the benefits at least offset the costs of disclosure, but do not disclose it when the costs outweigh the benefits [10]. For instance, by disclosing PHI about dietary habits, an mHealth app could provide users with personalized insights such as customized meal plans and improve health by encouraging better nutrition. Yet, users may also face costs, like privacy concerns arising from the possibility of unauthorized access or misuse of their PHI, such as being targeted by marketers for unhealthy food products based on their dietary habits. Users develop their disclosure behavior based on whether these benefits outweigh the associated costs, highlighting their systematic tradeoff between benefits and costs in relation to disclosure behavior [7]. Various benefits and costs have been used to explain disclosure behaviors in different contexts, such as mobile apps [43], e-commerce [7], and social networks [8] (see Table A1 in Appendix A).

Disclosure behaviors have largely been explained by drawing on a linear understanding of privacy calculus theory where benefits increase and costs decrease disclosure behavior independently [7,14]. That is, traditional privacy calculus theory often considers factors in isolation or assumes linear, additive effects. However, as privacy decisions become increasingly complex, there are indications that benefits and costs are not independent [44–46]. For instance, individuals with heightened privacy concerns tend to discount the benefits associated with information disclosure [46], while benefits can also reduce privacy concerns [23,47]. Recent research on the relationship between benefits and costs reveals that different combinations of them, so-called configurations, explain users' disclosure [48]. This is particularly helpful because not all users are alike, and these different combinations of benefits and costs can be equifinal, leading to the same disclosure behavior for various types of users [48]. Some users, for example, disclose their PHI to an mHealth app because they expect to gain health benefits and personalized insights and have no privacy concerns. Others may have privacy concerns but still disclose their PHI, relying on their trust in the mHealth app to manage the PHI appropriately and expecting to gain health benefits from its use. These different user types exemplify that the path to disclosure is not singular because different combinations of benefits and costs can be equifinal in leading to the same user behavior.

In addition, disclosure behavior depends on the temporal effects of benefits and costs [15,16]. More specifically, users determine their initial disclosure based on the expected benefits and costs [13,14]. They then determine their disclosure after initial disclosure, such as continuous disclosure, based on the experienced benefits and costs [15]. This suggests that users' behavior after initial disclosure is contingent upon two privacy tradeoffs together: one tradeoff based on expected benefits and costs before the initial disclosure and another based on experienced benefits and costs after it [15].

Extant privacy literature thus suggests that the benefits and costs of disclosure determine users' disclosure behavior. As extant work indicates that users update the benefits and costs after their initial disclosure [15] and that benefits and costs work together [48], we adopt a theoretical view on disclosure behavior that considers expectations and experiences together in the form of configurations. Drawing on this novel perspective of privacy calculus theory, we explain discontinuous disclosure – a new and distinct form of disclosure behavior – in the context of mHealth apps. While prior literature explains disclosure behavior in a variety of contexts, including mobile apps [43,46] and health [9,49], there is little knowledge about disclosure behavior in the context of mHealth apps, even though it represents a unique context with different characteristics. With PHI being highly sensitive, resulting in potentially higher privacy concerns [23], and mobile apps being able to reinforce the benefits (e.g., via tangible health benefits [37]), users weigh potentially higher costs against greater benefits in the mHealth app context. Consequently, there may be different dynamics between benefits and costs in this context compared to previous studies. In particular, previous work indicates that health benefits, personalization, trust, and privacy concerns are the primary drivers of users' disclosure in mHealth apps. Based on our conceptualization of these factors, we identify two types of positive drivers: (1) functional utilities (i.e., health benefits and personalization), which represent the direct positive outcomes related to the mHealth app's value proposition, and (2) trust as an enabling factor, which creates a safe interaction environment through confidence beliefs. Together, these positive drivers constitute the "benefits" side of the tradeoff in privacy calculus theory, which models disclosure as a calculation in which health benefits and personalization represent the core positive factors that motivate the user to disclose [13, 25], whereas trust serves to specifically mitigate the perceived costs [23]. Correspondingly, privacy concerns represent the "costs" side of this tradeoff, constituting the negative drivers that prevent disclosure.

3. Discontinuous disclosure

3.1. Related research on disclosure

Literature offers explanations for the reasons users initially disclose personal information [11], the reasons they initially do not disclose personal information [12], and the reasons they continue disclosing personal information [15], which we will outline next.

Initial disclosure describes the behavior in which users start disclosing their personal information [11]. This behavior is driven by users' positive tradeoff of expected benefits and costs (i.e., a tradeoff where the expected benefits outweigh the expected costs) [14]. For example, a user might start disclosing their PHI to an mHealth app when their expected benefits, such as receiving personalized meal plans, outweigh their expected costs, such as potential privacy concerns.

Initial non-disclosure describes the behavior in which users do not start disclosing their personal information [12]. This behavior is driven by users' negative tradeoff of expected benefits and costs (i.e., a tradeoff where the expected costs outweigh the expected benefits) [12]. For example, a user may choose not to disclose their PHI to an mHealth app because the expected costs, such as the potential for data misuse, outweigh the expected benefits of receiving personalized workout suggestions.

Continuous disclosure describes the behavior in which users keep disclosing their personal information over time [15]. This behavior is driven by users' positive tradeoff of expected benefits and costs prior to disclosure and their positive tradeoff of experienced benefits and costs after it. In both tradeoffs, the benefits outweigh the costs [15]. For this behavior, users compare their expectations with their experiences, driven by the alignment of the expected and experienced benefits and costs [15]. For example, after initially disclosing the PHI, a user finds the mHealth app's fitness advice to be helpful. Because this positive experience aligns with their initial expectations, they continue to disclose their PHI as the experienced benefits consistently outweigh any experienced costs.

While research focusing on these disclosure behaviors is established and has been used in different domains, such as e-commerce [7], online social networks [8], and health [9], it cannot explain situations in which users stop disclosing information after some time.

3.2. Discontinuous disclosure as a new disclosure behavior

We define discontinuous disclosure as the behavior in which users who initially disclose their personal information stop doing so after some time. Importantly, this involves a behavioral shift, as users, following an initial period of voluntary disclosure, deliberately choose to stop this disclosure, thereby reflecting not just a passive cessation but an active re-evaluation by the user. Because of this distinct behavioral shift, discontinuous disclosure emerges as a novel and unique disclosure behavior that differs from the established disclosure behaviors – initial disclosure, initial non-disclosure, and continuous disclosure (see Table 2) – in several ways and cannot be fully understood with existing theoretical explanations. It thus highlights a new, distinct path in the conceptual model of disclosure behaviors that represents the reversal from an initial state of disclosure back to non-disclosure (see Fig. 1).

To explain this behavioral shift, we suggest that discontinuous disclosure is driven by two divergent tradeoffs: a positive tradeoff of expected benefits and costs prior to disclosure, and a negative tradeoff of experienced benefits and costs after it. In the first tradeoff, the expected benefits outweigh the expected costs, leading to the initial disclosure. In the second tradeoff, occurring at a point after initial disclosure, the experienced costs outweigh the experienced benefits, leading to discontinuous disclosure. Crucially, this shift from a positive expected tradeoff to a negative experienced tradeoff is marked by a discrepancy between users' initial expectations and their subsequent experiences. In other words, users compare their initial expectations regarding benefits and costs before their initial disclosure with the actual benefits and costs they experience after this disclosure. If experiences fall short of expectations, or if unexpected negative consequences arise, this discrepancy triggers a re-evaluation of the experienced tradeoff, which may then become negative, ultimately leading users to discontinue their disclosure. For example, users might initially disclose their PHI to an mHealth

Table 2
Comparison of disclosure behaviors.

	Initial non-disclosure	Initial disclosure	Continuous disclosure	Discontinuous disclosure
Focus	Why users do not disclose personal information initially	Why users disclose personal information initially	Why users keep disclosing personal information over time	Why users stop disclosing personal information after initial period of voluntary disclosure
Considered benefits and costs	Expected benefits and costs	Expected benefits and costs	Experienced benefits and costs	Expected and experienced benefits and costs
Temporal effects	Not considered	Not considered	Alignment of expectations and experiences	Discrepancy of expectations and experiences
Tradeoff	Negative tradeoff of expectations	Positive tradeoff of expectations	Positive tradeoff of expectations aligns with positive tradeoff of experiences	Positive tradeoff of expectations shifts to negative tradeoff of experiences
Key factors	Equally positive and negative perceptions	Equally positive and negative perceptions	Primarily positive perceptions	Primarily negative perceptions
Theoretical mechanism	Expected negative outcome: judgment that costs will outweigh benefits	Expected positive outcome: judgment that benefits will outweigh costs	Confirmation of expectations: positive experiences align with and validate expectations	Violation of expectations: negative experiences create discrepancy that invalidates initial expectations
Examples in IS research	[12]	[11]	[15]	This study

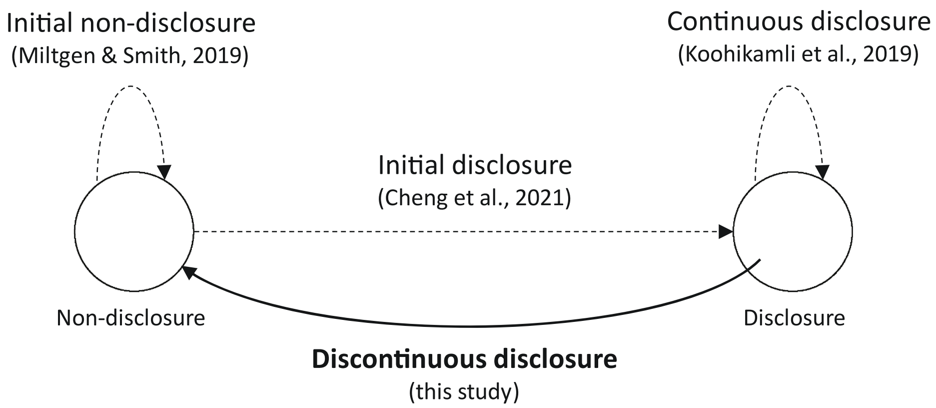

Fig. 1. Conceptual model of disclosure behaviors.

app, expecting to receive personalized health advice and believing their PHI will be handled appropriately. However, after this initial disclosure, a discrepancy might arise: the app may not deliver the personalized health advice they expected, or the users might discover that their PHI is used in ways they did not expect. This discrepancy triggers a negative re-evaluation of the experienced tradeoff, leading users to discontinue disclosure to avoid any negative consequences and regain a sense of control over their personal information [12,50].

Following this, we theorize that discontinuous disclosure is driven by heuristics or emotional evaluations, as users place greater weight on the costs and potential negative outcomes after initial disclosure, which results in a discrepancy between expectations and experiences. This is consistent with research suggesting that discontinuous behaviors inherently rely on different cognitive processes that are primarily driven by negative experiences [51]. This grounding in negative experiences is particularly relevant for discontinuous disclosure. Negative perceptions, such as privacy concerns, often emerge or intensify after the initial disclosure, since the potential negative consequences of disclosure are often delayed and may unfold at a later point in time [16,52]. The emergence of such privacy concerns after initial disclosure further illustrates that perceptions of benefits and costs may change over time [15,16,52]. Consequently, users may discontinue disclosure because their tradeoff of experienced benefits and costs becomes negative or insufficiently positive compared to the tradeoff of expected benefits and costs. In other words, users' negative experiences create a discrepancy with their initially more optimistic expectations, leading them to discontinue their disclosure.

Discontinuous disclosure therefore shifts the focus from a static, one-time tradeoff to a dynamic perspective that accounts for how perceptions may change over time, making it conceptually distinct from other disclosure behaviors (see Table 2). Initial disclosure and non-disclosure solely hinge on a one-time tradeoff based on expectations [11,12]. Discontinuous disclosure, however, like continuous disclosure [15], incorporates both the tradeoffs based on expectations and experiences. Yet, it is the discrepancy between these expectations and experiences that fundamentally separates them.

While continuous disclosure is primarily driven by positive experiences where users' experiences align with or confirm their initial expectations [15], which is consistent with suggestions from broader IS research that continuous behaviors stem from the alignment between users' expectations and their actual experiences [53,54], discontinuous disclosure arises from a discrepancy between them. Essentially, users' experiences fall short of, or negatively deviate from, initial positive expectations, which can trigger a re-evaluation that leads to a negative experienced tradeoff and a behavioral shift from their initial voluntary disclosure to a deliberate choice to discontinue it. For example, one user might initially expect an mHealth app to provide personalized health advice and find that their experiences align with these expectations, leading to a positive experienced tradeoff and continuous disclosure. Another user, with similar initial expectations, might find the app's advice generic or become concerned about privacy after an update. This discrepancy between their positive initial expectations and less favorable experiences can trigger a negative re-evaluation of the experienced tradeoff, leading them to discontinue disclosure.

To explain discontinuous disclosure and the behavioral shift it represents, it is crucial to understand the discrepancy between users' expectations and experiences. Explaining this discrepancy requires considering expected and experienced benefits and costs together, rather than analyzing experienced tradeoffs in isolation, as is common in extant literature [15]. With discontinuous disclosure, expectations form the baseline upon which users then weigh their subsequent experiences to determine whether to discontinue disclosure based on both tradeoffs together. If this baseline of initial expectations is not met by subsequent experiences – for instance, if promised benefits do not materialize or unforeseen costs arise – a discrepancy emerges. This discrepancy can then trigger a negative re-evaluation of the experienced tradeoff, ultimately leading to discontinuous disclosure. In sum, this perspective, which explains how users reverse their initial choice to disclose, requires a theoretical model that explicitly accounts for this dynamic process. We outline this model next.

3.3. Toward an understanding of discontinuous disclosure

To explain discontinuous disclosure, we developed a two-step research model that integrates an initial tradeoff based on expectations with a subsequent one based on experiences (see Fig. 2). We theorize that this behavioral shift is triggered by a discrepancy between these stages. This sequential logic is fundamental: users must first form expectations before they can assess whether those expectations are met, making the initial tradeoff a necessary prerequisite for the subsequent evaluation of experiences.

Following prior research that suggests that benefits and costs work together in configurations [48], we deliberately balance model parsimony with explanatory sufficiency. Although a more parsimonious model might aggregate health benefits and personalization into a single second-order benefits construct, this would mask the very discrepancies central to our theory.

Similarly, to uncover the various distinct pathways that lead users to discontinue disclosure, the analysis must move beyond assessing independent "net effects" to instead uncover their combinatorial logic. For

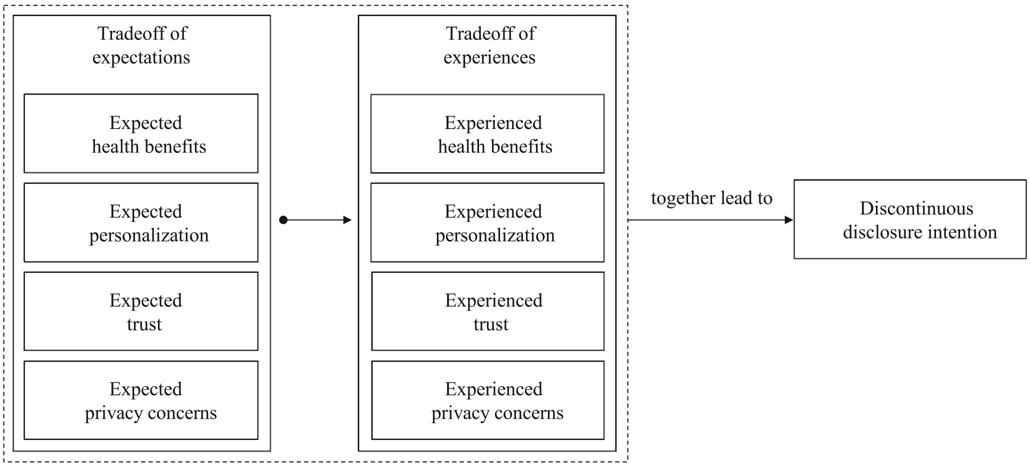

Fig. 2. Research approach.

instance, a lack of trust may be the decisive factor for one user, whereas for another, it might be the failure to experience tangible health benefits, even if they still trust the mHealth app. In sum, this granular, configurational two-step approach is therefore essential to uncover the distinct causal recipes characterizing these different pathways. This analysis is explained in more detail next.

4. Method

Although there are indications that benefits and costs work together [48], privacy calculus theory does not provide detailed guidance on their precise relationship. For this reason, we adopted an inductive approach to empirically uncover the relationship between expected and experienced benefits and costs and discontinuous disclosure, allowing us to identify patterns and generate insights directly from the data rather than testing pre-existing hypotheses for which privacy calculus theory provides limited guidance. Specifically, we use two-step fsQCA [17] to inductively uncover the various configurations, that is, the specific combinations of expected and experienced benefits and costs that explain discontinuous disclosure. This two-step variant of fsQCA is particularly well-suited for our study, as it enables us to model the sequential nature of our theoretical argument: initial expectations form a baseline (Step 1) upon which users then weigh their subsequent experiences (Step 2) to determine whether to discontinue disclosure based on both expectations and experiences together. We explain our approach in more detail in the following.

4.1. Data collection

We collected data from 322 users who had recently started disclosing PHI to an mHealth app, capturing expectations and experiences simultaneously. Although a longitudinal design may allow for more direct observation of potentially changing perceptions, this retrospective approach using cross-sectional data is well-suited for our study for two main reasons. First, it is a well-established approach for the initial stages of theory development and validation, a practice consistent with foundational post-adoption research in IS [54]. Second, it is particularly appropriate for models grounded in an expectation-experience discrepancy, and a common practice in IS [53,54].

Nevertheless, this design requires careful consideration of potential recall biases: users' initial expectations may degrade over time due to memory decay, or they might subconsciously align recalled expectations with their experiences, a problem known as backward assimilation [55]. To counteract these potential biases, our design incorporates two primary remedies. First, prior research shows that salient past events are more likely to be remembered, thereby enhancing the accuracy of recall [56]. In line with this, we anchor our measurement to the user's initial decision to start disclosing PHI, a distinct and salient event that provides a reliable cognitive reference point. Second, our design shortens the recall period by recruiting only participants who had started disclosing PHI to an mHealth app within the past four weeks, ensuring the event was recent and thus minimizing the potential for memory decay or backward assimilation. Together, this combination of a recent and salient event provides a robust foundation for our analysis because it enhances the reliability of the recalled expectations that serve as the baseline for our model.

We then conducted an online survey via the established panel provider Prolific [57], whose participants are more likely to provide meaningful answers compared to other panel providers [58], which yields higher data quality [59]. To identify eligible participants, we administered an initial screening survey, in which we asked participants from the United States whether they had started disclosing their PHI to an mHealth app in the past four weeks. Those who met the specified criteria were subsequently invited to participate in a follow-up survey. Survey participation was anonymous, reducing the likelihood of participants feeling obligated to respond to the survey in a manner they perceive as desirable, thereby mitigating common method bias [60]. We compensated the participants with US$11.50, which is above the U.S. minimum wage. Details on the participant screening and exclusion criteria, along with the demographics of the final sample, can be found in the Appendix (see Table B1 in Appendix B).

4.2. Measurement and validation

To capture users' expected and experienced benefits and costs and their discontinuous disclosure intention in the context of mHealth apps, we adapted well-established constructs validated in prior research (see Table C1 in Appendix C).

We measured expected benefits and costs retrospectively, while experienced benefits and costs were measured at the time of survey completion. For the benefits, we used three items each to measure expected and experienced health benefits [25], personalization [13], and trust [26]. For the costs, we used four items for expected and experienced privacy concerns [7].

To assess discontinuous disclosure, we measured discontinuous disclosure intention. This aligns with the predominant approach in privacy calculus research, which widely relies on intention as a proxy for behavior (see Table A1 in Appendix A). This focus is also well-grounded in behavioral research. Discontinuous disclosure is not a passive cessation but a planned, deliberate behavioral shift resulting from a user's conscious re-evaluation. For such reasoned actions, foundational models establish intention as the most direct cognitive antecedent, capturing the decision that precedes the action itself [61]. Since our model explains the cognitive re-evaluation that results in this decision, intention is the most appropriate construct to capture this outcome. Accordingly, we used three adjusted items based on established measures of initial disclosure intention [9] to measure discontinuous disclosure intention because both initial and discontinuous disclosure involve a distinct decision point that precipitates a change in disclosure behavior. Our adaptation specifically shifted the items' focus from an intention to start disclosing to the intention to stop the ongoing disclosure, thereby representing a targeted change in the direction of action. For instance, we adapted the item "I am likely to reveal my health information in this online health community" to "I am likely to stop revealing my personal health information in {APP}." We evaluated all measurement items using a seven-point Likert scale, ranging from "strongly disagree" (1) to "strongly agree" (7).

As recommended for fsQCA studies [62], we validated the measurement model by ensuring content validity, indicator reliability, construct reliability, and discriminant validity. We established content validity by adopting well-established measures from previous research and adapting them to the context of mHealth apps (see Table C1 in Appendix C). For indicator reliability, we checked the item loadings and excluded two items each from the expected and experienced health benefits due to loadings below 0.707. The loadings of all remaining items exceed 0.707, indicating indicator reliability [63]. To ensure construct quality, we confirmed that composite reliability exceeds the value of 0.70 and average variance extracted (AVE) surpasses 0.50 (see Table D1 in Appendix D) [64]. We included the square root of AVE in the diagonal of the bivariate correlations to ensure discriminant validity, as it describes the extent to which an item differs from other items [65]. Because the square root values in the diagonal exceeded the corresponding construct correlations (see Table D1 in Appendix D), we attest no issues with discriminant validity [64]. Additionally, we employed the heterotrait-monotrait (HTMT) ratio of correlations to evaluate discriminant validity [66]. The HTMT ratio is 0.74, which is lower than the $HTMT_{0.85}$ criterion and thus indicates discriminant validity. We also ensured that common method bias does not exert a distorting influence on the results (see Appendix D). We conclude that our measurement model is valid and proceed with the analysis.

4.3. Data analysis using two-step fsQCA

To examine users' discontinuous disclosure, we employed an fsQCA [17]. Grounded in set theory, fsQCA examines the relationship between configurations of conditions and an outcome [67]. While a condition reflects a set membership in a variable, a configuration represents a combination of conditions related to an outcome [62], often referred to as a causal recipe. It moves beyond analyzing the net effects of isolated factors and instead focuses on how these configurations of conditions, as a whole, are linked to the outcome, through how the conditions work together [62,68]. This approach allows for an understanding of causal complexity, where the relevance or impact of one condition is often contingent upon other conditions within the configuration, and equifinality, where different configurations can result in the same outcome [67–69].

The two-step approach further separates the analysis into two distinct steps, offering a key advantage over conventional fsQCA by further distinguishing between remote and proximate conditions [17]. This approach allows for accounting for differing temporal and causal distances from the outcome: remote conditions are temporally and causally more distant, while proximate conditions are closer to it [70]. In Step 1, the analysis focuses on identifying the necessary context formed by the remote conditions. The purpose of this step is to determine if a specific configuration of these remote conditions is a prerequisite, meaning it must consistently be present for the outcome to occur. If such a context is identified, it establishes the foundational baseline for the sufficiency analysis in Step 2. Importantly, this analysis of necessity is applied exclusively to the remote conditions to identify this required starting point for the causal process. Step 2 then shifts to the proximate conditions, which are analyzed alongside this identified necessary context to determine how they together lead to the outcome, resulting in sufficient configurations [17]. In other words, the two-step approach recognizes that the influence of proximate conditions can be contingent upon the broader context established by remote conditions [17,70].

In this study, the expected benefits and costs are the remote conditions, the experienced benefits and costs are the proximate conditions, and discontinuous disclosure intention is the outcome. The rationale for this assignment stems from our proposed theoretical model, specifically the temporal and causal ordering of users' perceptions: expectations, captured as benefits and costs before the initial disclosure, inherently form the baseline against which subsequent experiences are assessed. This inherently positions the expected benefits and costs as temporally and causally more distant from discontinuous disclosure intention, making them remote conditions.

Consequently, this specific theoretical assignment of conditions allows for examining how the combined consideration of initial expectations and subsequent experiences, with their respective benefits and costs, ultimately leads to discontinuous disclosure intention. All analyses were performed using the QCA package for R [71]. We provide a detailed description of our approach in Appendix E and a summary of the two steps in Table 3.

5. Results

Using this configurational approach, we identified one necessary context for discontinuous disclosure intention consisting of expected health benefits and expected personalization (consistency = 0.91, coverage = 0.60; relevance of necessity = 0.51) in Step 1. We did not identify expected trust and expected privacy concerns as necessary, indicating they are not relevant for discontinuous disclosure intention [17] (see Table 4). Because the identified necessary context involves both expected health benefits and personalization, we name it "personalized health benefits," as it highlights that personalization and

Table 3
Two-step fsQCA [17].

	Step 1	Step 2
Type	Analysis of necessity	Analysis of sufficiency
Goal	Identify necessary context for the outcome	Identify sufficient configurations that lead to the outcome
Role	Reveal the baseline for subsequent outcome to occur (i.e., the necessary context for discontinuous disclosure intention)	Explain the outcome when combined in specific configurations, together with the identified necessary context from Step 1
Conditions analyzed	All remote conditions (here: expected health benefits, expected personalization, expected trust, expected privacy concerns)	Necessary context condition(s) identified in Step 1 and all proximate conditions (here: expected health benefits, expected personalization, experienced health benefits, experienced personalization, experienced trust, experienced privacy concerns)
Relation to outcome	Identified necessary context must be present for the outcome to occur	Identified sufficient configurations are sufficient for the outcome to occur

Table 4
Sufficient configurations.

		The privacy-conscious realist	The privacy-conscious skeptic	The trustful skeptic	The privacy-conscious distruster
Tradeoff of expectations	Expected health benefits	●	●	●	●
	Expected personalization	●	●	●	●
	Expected trust				
	Expected privacy concerns				
Tradeoff of experiences	Experienced health benefits		⊗	⊗	
	Experienced personalization	⊗			●
	Experienced trust	●		●	⊗
	Experienced privacy concerns	●	●		●
	Raw coverage	0.45	0.46	0.44	0.52
	Unique coverage	0.02	0.03	0.04	0.07
	Consistency	0.88	0.91	0.87	0.87
	Solution coverage	0.63			
	Solution consistency	0.84			

Note: Black circles ● indicate the presence of a condition, white crossed-out circles (⊗) indicate the absence of a condition, and blank spaces () indicate "don't care" situations. In these cases, the specific conditions are irrelevant to the configuration and can be present or absent.

health benefits are necessary together.

Including this necessary context in Step 2, we revealed four sufficient configurations, illustrating the different pathways that lead users to develop an intention to discontinue disclosure. We provide a graphical representation in Table 4.

The results show that the intention to discontinue disclosure arises not from expected or experienced factors in isolation, but from their sequential processing. More specifically, the expected benefits and costs form the necessary context upon which the experienced benefits and costs are evaluated. Because the necessary context is a mandatory part of every sufficient configuration, this means that all users with a discontinuous disclosure intention expect health benefits and personalization from mHealth apps. They then weigh the experienced benefits and costs upon this baseline, such that four different configurations lead them to discontinuous disclosure intention.

The first configuration describes *privacy-conscious realists* who experience trust in the mHealth app after the initial disclosure but also privacy concerns and experience that the app lacks personalization, representing users with a realistic, unprejudiced tradeoff. The second configuration describes users who experience no health benefits but privacy concerns after initial disclosure, which we call *privacy-conscious skeptics* to highlight their skepticism towards the mHealth app and its promises. The third configuration describes *trustful skeptics* who trust the mHealth app but still intend to discontinue their PHI disclosure because of a lack of experienced health benefits, regardless of experienced personalization or privacy concerns. The fourth configuration describes users for whom experienced health benefits are irrelevant and whose expectation for personalization is met but intend to discontinue disclosure because of experienced privacy concerns and lack of trust. Accordingly, we refer to them as *privacy-conscious distrusters*.

We evaluated our findings based on raw coverage and unique coverage. The raw coverage describes the extent to which a configuration covers the outcome [69,72]. For the four identified sufficient configurations, this ranges from 0.44 to 0.52, indicating high explanatory power. The unique coverage indicates the extent to which a configuration covers the outcome, excluding the proportions that are covered by other configurations [69]. It ranges from 0.04 to 0.07, suggesting that each sufficient configuration uniquely contributes to explaining discontinuous disclosure intention.

We assessed the solution's overall quality based on the solution coverage that measures the extent to which all four sufficient configurations together explain the outcome [69,72], yielding a value of 0.63. To evaluate the extent to which all configurations together consistently explain discontinuous disclosure intention, we draw on the solution consistency, which is 0.84 and exceeds the recommended minimum threshold of 0.75 [72]. Overall, our solution has adequate explanatory power [62,73]. Furthermore, the solution proved robust across a series of sensitivity analyses testing key analytical parameters (see Appendix F).

6. Discussion

Many users discontinue the disclosure of their PHI due to privacy concerns [3], foregoing potential health benefits. Our results reveal four configurations of expected and experienced benefits and costs that together explain users' discontinuous disclosure intention. Building on these empirically identified configurations, we next explain the theoretical mechanisms behind this new disclosure behavior and derive propositions from them. Finally, we discuss the implications for research and practice.

6.1. Theoretical mechanisms underlying discontinuous disclosure

To advance existing literature on privacy-related disclosure behavior, we develop five propositions that explain the underlying cognitive and perceptual mechanisms that result in discontinuous disclosure. To achieve this, we draw upon the empirical configurations identified through our fsQCA (see Table 4) to explain how specific combinations of expected and experienced benefits and costs lead to discontinuous disclosure intention. This approach is particularly suited to theorizing such behavioral reversal, as it allows capturing how specific combinations of factors result in discontinuous disclosure without privacy calculus theory specifying how these factors are related [68,74]. For this reason, the following propositions aim to specify how exactly expected and experienced benefits and costs work together to explain discontinuous disclosure in the context of mHealth apps. We will begin with the results of Step 1 of the fsQCA, that is, the necessary context.

Before the initial disclosure of PHI to an mHealth app, users seek personalization and health benefits, both of which are important individual drivers of disclosure behavior [9,13,25]. Our findings reveal a refinement to this isolated understanding in the context of discontinuous disclosure by showing that the combination of expected personalization and health benefits is necessary for users' discontinuous disclosure intention of PHI (see Table 4). More specifically, this combined expectation acts as a cognitive anchor, establishing the initial baseline against which users assess their experiences. If users' experiences with the mHealth app fail to meet this baseline, that is, if they perceive that the app does not deliver the expected personalized health benefits, a discrepancy emerges. This unmet expectation, regardless of users' expected trust or privacy concerns, then serves as a primary trigger for the re-evaluation process that can prompt an intention to discontinue disclosure. Although this violation of the initial baseline is the unifying trigger across all configurations, different patterns of post-disclosure experiences ultimately shape this re-evaluation process. We suggest the following proposition (P):

P1: Users must expect health benefits and personalization prior to the initial disclosure to have a discontinuous disclosure intention thereafter.

Privacy-conscious realists prioritize their experienced privacy concerns and the lack of personalization over potential health benefits, despite their trust in the mHealth app. While they trust the mHealth app, privacy concerns and the lack of personalization after the disclosure are more important for them, leading to discontinuous disclosure intention irrespective of potential health benefits. It has been shown that trust decreases privacy concerns [75] and that privacy concerns decrease trust [26]. Extending prior insights, we reveal that some users experience trust and privacy concerns simultaneously, reflecting a state of privacy ambivalence, where users hold conflicting perceptions at the same time. Users may be aware that misuse of their PHI is possible but still trust the mHealth app to handle their personal information responsibly. This means that despite trusting an mHealth app, privacy concerns may still arise, as PHI is more sensitive than other types of information [23]. Together with the lack of experienced personalization they expect from the mHealth app, this creates a discrepancy, leading to a re-evaluation of their experienced tradeoff that, if negative, prompts the intention to discontinue disclosure. We therefore propose:

P2: Users who expect health benefits and personalization and experience privacy concerns and trust but no personalization have a discontinuous disclosure intention.

Privacy-conscious skeptics experience privacy concerns and a lack of health benefits. Initially, they expected health benefits and personalization when disclosing their PHI to an mHealth app, but the lack of experienced health benefits after initial disclosure lets them develop a discontinuous disclosure intention. Experienced personalization is not relevant for them, indicating that the health benefits outweigh personalization for these users. This aligns with existing literature showing that health benefits are crucial for users to disclose PHI [25,49] and that the primary goal of health services like mHealth apps is to provide health benefits [9]. If an mHealth app fails to meet this goal and does not provide any health benefits, users may view it as ineffective and not worth disclosing their PHI and risking compromising their privacy. Consequently, as health benefits often need to outweigh privacy concerns for disclosure to occur [9,49], the discrepancy arising from the lack of experienced health benefits, when combined with ongoing privacy concerns, leads to a re-evaluation where the experienced tradeoff is no longer positive, prompting the intention to discontinue disclosure. We propose:

P3: Users who expect health benefits and personalization and experience privacy concerns but no health benefits have a discontinuous disclosure intention.

Trustful skeptics are similar to privacy-conscious skeptics in that they also do not experience health benefits. Unlike privacy-conscious skeptics, trustful skeptics have trust in the mHealth app after initially disclosing their PHI but still develop an intention to discontinue disclosure. This trust may be attributed to differences in how users assess the transparency of mHealth apps regarding their handling of PHI, with higher transparency ratings increasing trust [29,75]. Once this trust is established, privacy concerns become less significant, as trust mitigates these concerns [75,76]. However, despite this experienced trust, the main driver for using mHealth apps often lies in gaining health benefits [9,18]. The experienced lack of these expected benefits creates a state of cognitive dissonance [77], as their belief in the app's trustworthiness clashes with the reality of its poor performance. The decision to resolve this dissonance by discontinuing disclosure is theoretically crucial when contrasted with privacy-conscious skeptics. It demonstrates that trust alone is insufficient to retain users and highlights the dominance of goal-disconfirmation: even when privacy concerns are low, the violation of the app's core value proposition triggers a negative re-evaluation. Thus, we propose:

P4: Users who expect health benefits and personalization and experience trust but no health benefits have a discontinuous disclosure intention.

Privacy-conscious distrusters share similarities with privacy-conscious realists, as they also do not prioritize health benefits after their initial disclosure. The lack of trust after initial disclosure, together with privacy concerns, leads to discontinuous disclosure intention, even when personalization is experienced and regardless of any experienced health benefits. Privacy-conscious distrusters experience privacy concerns but no trust in the mHealth app. This might be due to privacy concerns reducing their trust [26], with the high sensitivity of PHI further increasing privacy concerns [23]. Notably, privacy-conscious distrusters are the only configuration where expectations and experiences partially align (as per P1) but still develop a discontinuous disclosure intention: they expect personalization before the initial disclosure, which they also experience after disclosure. However, while they experience personalization, it does not outweigh their simultaneously experienced privacy concerns. This triggers a re-evaluation of their experienced tradeoff. Although an expected benefit of the necessary context is delivered in the form of personalization, the absence of trust increases the perceived weight of their privacy concerns. This results in a discrepancy between the positive aspect of receiving a desired personalized service and the negative perception of privacy concerns and lack of trust. As such, in this re-evaluated tradeoff, the key premise of privacy calculus theory – that the benefits of disclosing personal information must outweigh the costs for users [10] – is not fulfilled. This failure of experienced personalization to sufficiently compensate for high privacy concerns can be attributed to users' increasing awareness that personalized services necessitate extensive data collection and processing, which often heightens anxiety about the potential misuse of their data [52]. This dynamic also illustrates the crucial role of trust as an enabling factor [7,23]: the experienced functional utility of personalization fails precisely because the psychological security needed to accept the associated data processing risks is missing when trust is absent. While one might consider regret theory [78], the mechanism here seems less about past decisions and more about a forward-looking re-evaluation where the perceived risks, amplified by a lack of trust, decisively outweigh the single experienced benefit of personalization. This negative re-evaluated tradeoff, in turn, prompts the intention to discontinue disclosure, such that we propose:

P5: Users who expect health benefits and personalization and experience personalization and privacy concerns but no trust have a discontinuous disclosure intention.

Synthesizing the mechanisms across these configurations, a practice common in configurational theory-building [79], reveals a more structured explanation for discontinuous disclosure. Two overarching mechanisms emerge, showing that while the trigger is always a discrepancy with the initial baseline (see P1), the nature of that discrepancy differs fundamentally. The first mechanism is rooted in benefit realization (see P3 and P4). It is triggered by the mHealth app's failure to deliver its core value proposition, demonstrating the dominance of goal disconfirmation. The second mechanism centers on process integrity (see P2 and P5). The trigger is a breakdown in the data-for-service exchange itself, such as a lack of trust or emerging privacy concerns, irrespective of any health outcomes. Essentially, the four configurations therefore manifest two overarching types of failure, corresponding to (1) a rational failure of the app's core value proposition, where the expected benefits simply do not materialize, and (2) a normative failure in the integrity of the data exchange process itself, where a breakdown in trust or heightened privacy concerns outweigh the app's utility. While the rational failure aligns with traditional privacy calculus theory, as it reflects a simple cost-benefit tradeoff [12,13], the normative failure aligns with recent work suggesting that in AI-driven contexts like mHealth apps, the privacy concerns are increasingly rooted in fears of AI misuse (e.g., AI-deduced disclosure or algorithmic bias) [6,12,80].

6.2. Theoretical implications

Our study makes several contributions to privacy research, privacy calculus theory, and mHealth app literature by explaining why users discontinue disclosing their PHI to mHealth apps.

First, we contribute to privacy research by conceptualizing and defining discontinuous disclosure as a novel and theoretically distinct disclosure behavior. While extant literature extensively covers initial disclosure [13], initial non-disclosure [12], and continuous disclosure [15], it offers limited explanation for why users, who initially shared PHI voluntarily, deliberately reverse this choice. We address this by conceptualizing discontinuous disclosure as the result of an inherent behavioral shift: a deliberate re-evaluation of the initial decision to disclose, prompted by a perceived discrepancy between initial positive expectations and subsequent, often less favorable, experiences. Before disclosing their PHI, users generally perceive a positive tradeoff between expected benefits and costs, which motivates their initial disclosure (see P1). After their initial disclosure, this positive tradeoff can shift into a negative one if their experiences do not meet these expectations (see P2-P5). This shift is largely due to negative experiences that emerge after initial disclosure, as potential negative consequences of disclosure are often delayed and may unfold at a later point in time [16,52]. When users encounter such a discrepancy between their expectations and experiences, this misalignment triggers a cognitive re-evaluation, prompting them to discontinue disclosure (i.e., actively reversing their prior choice to disclose). With this, we advance privacy research by positioning discontinuous disclosure as a novel disclosure behavior, offering an explanation for how and why users actively reverse their initial disclosure decision, even at the expense of potential health benefits.

Second, by developing this explanation, we contribute to privacy calculus theory by shifting the focus to a dynamic, temporally structured perspective that explicitly incorporates the discrepancy between users' initial expectations and their subsequent experiences to explain discontinuous disclosure. While traditional applications of privacy calculus theory often focus on a static, one-time tradeoff for initial disclosure [11,14], and studies on continuous disclosure introduce temporal effects [15], we emphasize how a mismatch between these temporal steps can trigger a behavioral shift. We show that discontinuous disclosure results from the interaction between users' expectations and their experiences, especially when these diverge. Specifically, we reveal that users' tradeoff of expectations is crucial for discontinuous disclosure, as it represents the necessary context against which subsequent experiences are evaluated (see P1). In other words, it forms the baseline upon which the tradeoff of experiences leads to the actual discontinuous disclosure. Essentially, discontinuous disclosure is prompted when this baseline is not met by the subsequent experiences, initiating a discrepancy-driven re-evaluation process where the initially positive tradeoff shifts into a negative one, for instance, if expected benefits are not realized or unexpected costs, such as heightened privacy concerns, emerge. Consequently, explaining discontinuous disclosure requires moving beyond an isolated consideration of the experienced benefit-cost tradeoff. Instead, it necessitates a sequential and comparative view that recognizes how expectations serve as reference points for evaluating subsequent experiences. This reconceptualization advances privacy calculus theory [13,48] by moving from a static to a dynamic understanding that captures how benefits and costs interact within users' expectations, within their experiences, and across them.

Third, we contribute to privacy calculus theory by employing a configurational approach that reveals the complex and contingent causal structures underlying discontinuous disclosure, thereby extending the theory's application to behavioral reversals. While prior research has applied configurational thinking to explain initial disclosure using privacy calculus theory [48], our study advances this line of inquiry by focusing on the distinct dynamics of discontinuous disclosure. We show that this choice to discontinue disclosure is not driven by isolated factors operating in a linear fashion, but rather by a two-step process in which interdependent combinations of expected and experienced benefits and costs work together, with expectations forming the baseline against which the subsequent experiences are evaluated. This aligns with configurational literature, which posits that outcomes often arise from specific combinations of factors rather than their independent net effects [68,74]. The interactions within these configurations reveal specific interdependencies [81]. For instance, we reveal multiple layers of contingency: the influence of experienced trust is conditional on the broader configuration (see P2, P4, and P5), and the initial tradeoff of expectations (P1) itself acts as a foundational contingency for the entire process. For instance, the absence of experienced trust contributes to discontinuous disclosure, despite the presence of some experienced benefits (see P5). This highlights the enabling role of trust, operating not merely as another direct functional utility users expect, but as a foundational contingency that can alter the entire logic of the user's tradeoff. Conversely, we show that trust's positive influence is not absolute, as its presence can prove insufficient to retain users if other expected functional utilities are not met or privacy concerns emerge (see P2, P4). Finally, our identification of the four sufficient configurations (see P2-P5) underscores the principle of equifinality, which means that there are multiple, distinct pathways through which users, with varying perceptions regarding benefits and costs, arrive at the same outcome, that is, the intention to discontinue their PHI disclosure. This moves beyond generalized explanations by showing that user subgroups experience discontinuous disclosure through divergent experiential profiles and tradeoff logics. By highlighting the interplay of causal complexity, equifinality, and configurational contingency, our study provides a more nuanced theoretical account of how privacy calculus theory operates in the context of reversed disclosure decisions.

Fourth, we contribute to mHealth app literature by explaining disclosure behavior in this domain, extending privacy calculus theory to a highly sensitive and understudied health technology context. In mHealth settings, a distinct tradeoff arises: users weigh high potential benefits, such as improved health outcomes [18,19], against equally high costs, particularly privacy concerns stemming from the sensitivity of PHI [23]. Consistent with IS research on discontinuous behaviors, which suggests that individuals tend to prioritize negative perceptions [51], we find that privacy concerns that emerge or intensify after initial disclosure are especially influential for discontinuous disclosure to trigger a re-evaluation of the initial disclosure decision, a dynamic that our configurational two-step approach is particularly well-suited to capture because it is designed to reveal how combinations of factors, rather than their net effect, lead to an outcome. At the same time, personalized health benefits emerge as the critical baseline, as users expect mHealth apps to deliver on their core functionality of providing tailored health services (see P1). When these expectations are not met, or when privacy concerns grow salient, users re-evaluate their experienced tradeoff. If this re-evaluation results in perceived costs outweighing benefits, users are likely to discontinue disclosure, a shift consistent with findings that individuals are more sensitive to losses or threats than to potential gains [51]. By revealing the specific configurations of expected and experienced benefits and costs that jointly lead to discontinuous disclosure, our study provides a context-sensitive and theoretically grounded account of disclosure behavior in the mHealth domain.

6.3. *Practical implications*

Our results guide providers of mHealth apps on how to design and promote their applications to prevent users from discontinuing their disclosure of PHI, thereby helping them maintain user engagement and access to valuable user data. We offer practical guidance on how to effectively balance users' perceived benefits and costs when disclosing PHI. Specifically, our research reveals that users' intention to discontinue disclosing their PHI is shaped by how their initial expectations, especially personalized health benefits, are weighed against their subsequent experiences with the app's actual benefits and costs. To prevent discontinuous disclosure, mHealth app providers should therefore manage both user expectations and their subsequent experiences. This requires a dual focus: while providers must deliver on the promised functional utility, such as personalized health insights, they must simultaneously build and maintain trust as the foundational enabling factor that makes users willing to disclose their data in the first place.

Because users initially disclose PHI expecting personalized health benefits, providers must deliver on this promise and ensure these expectations are met. This means they must design apps that not only offer generic health monitoring, but also provide tailored insights, feedback, and actionable recommendations that users perceive as directly beneficial and relevant to their individual health goals. For instance, instead of general functions such as tracking steps, an mHealth app could offer tailored workout adjustments based on detected fatigue or activity levels or provide personalized dietary plans that adapt to weekly calorie burn, visibly demonstrating direct health improvements. Implementing features like progress dashboards that show long-term health trends or gamified health challenges with personalized milestones can further reinforce these experienced benefits, thereby aligning them with initial expectations. Beyond delivering personalized health benefits, establishing trust and mitigating privacy concerns are important for preventing discontinuous disclosure. For this purpose, providers should implement and clearly communicate robust privacy and security measures, such as end-to-end encryption for PHI, transparent data usage policies presented in accessible formats like interactive privacy dashboards, or specific user controls for their PHI disclosure, such as selective disclosure options allowing them to choose which particular PHI is disclosed. Finally, providers should adopt Ethical and Privacy by Design principles by embedding privacy safeguards into the app's development and consider regular third-party security audits.

Our findings further reveal different user types that intend to discontinue disclosure, indicating that a one-size-fits-all approach is insufficient and that providers should instead consider customized strategies for different users. To identify these user types in practice, mHealth app providers could employ various techniques to gather information about the users, including user profiling through onboarding questions or advanced data analytics techniques such as machine learning to automatically segment users based on their preferences and behaviors. Once identified, providers can then implement targeted interventions. For users experiencing trust and privacy concerns but lacking personalization (privacy-conscious realists), features clearly linking disclosed PHI to personalized insights are key, for instance, adaptive meal plans explaining suggestions based on user data, with customization options. Conversely, for those with privacy concerns and no experienced health benefits (privacy-conscious skeptics), providers must demonstrate tangible health improvements via simple reports alongside clear security and privacy information. Users experiencing trust but no health benefits (trustful skeptics) need features that directly convert PHI into clear health benefits, such as advanced analytics suggesting optimal bedtimes based on sleep and activity. Last, for those experiencing personalization and privacy concerns but a lack of trust (privacy-conscious distrusters), providers should implement visible trust-building elements like privacy dashboards detailing data use with opt-out options, and display security certifications to demonstrate corporate digital responsibility.

In addition to addressing the user types for discontinuous disclosure, we identified one user type associated with the absence of this intention: users who experience high trust and the absence of privacy concerns (see Table E2 in Appendix E). To foster this desired state among users and promote continuous disclosure, providers should reinforce data security, such as by using multi-factor authentication, provide clear and regular updates on privacy practices, such as monthly privacy reports detailing data use, and ensure the app delivers its core functionality without compromising users' privacy. Understanding these reasons also informs tailoring re-engagement strategies, such as personalized notifications highlighting new features that address a user's specific prior concern, such as new privacy controls for a user lacking trust.

6.4. *Limitations and future research*

Our study has several limitations. We rely on discontinuous disclosure intention to measure discontinuous disclosure. While using intention is an established method for measuring disclosure behavior (see Table A1 in Appendix A), we acknowledge that intention does not always translate into actual behavior [61]. However, unlike typical initial intentions, which are based on abstract positive expectations, the intention to discontinue disclosure is a corrective decision based on direct, often negative personal experiences. Such an experience-driven intention is likely held with greater conviction and thus may be less susceptible to the classic intention-behavior gap [61,82]. Still, future research should aim to capture users' actual discontinuous disclosure behavior alongside their intentions. This would allow for a direct test of whether these corrective intentions exhibit a stronger link to behavior, thereby providing more direct insights into the user's actual behavioral shift.

Similarly, while the retrospective approach to capturing users' initial expectations regarding benefits and costs is an established method in prior IS research [53,55], it inherently relies on accurate recall and may therefore not perfectly reflect users' true perceptions at the time of initial disclosure. Although we tried to mitigate this risk by anchoring our measurement to the salient event of a user's initial disclosure and by ensuring a short time frame of four weeks between this event and data collection, it still restricts the ability to directly observe the precise temporal evolution of users' perceptions of benefits and costs and the exact point of behavioral reversal from disclosure to discontinuous disclosure. To address this, future research should adopt longitudinal designs that measure expectations and experiences at multiple time points (e.g., tracking changes over weeks or months) or employ experimental methods drawing on behavioral tracking data (e.g., time-stamping disclosure decisions). These alternative designs would allow for a more precise understanding of the dynamic process, capturing not only actual behavior with greater accuracy but also how users' expectations truly evolve over time and turn into experiences.

We also did not consider individual differences such as users' age. As elders tend to have greater privacy concerns but may also benefit more from mHealth apps [47], future research should investigate this privacy-age dilemma from a configurational perspective of privacy calculus theory, as both the benefits and costs may be greater for elderly people, such that different configurations could emerge. Additionally, users' experience with previous privacy invasions may make them more sensitive to privacy concerns [13,25], so they are more likely to discontinue disclosing their PHI despite potential benefits. Drawing on theoretical perspectives that consider prior experience (e.g., habituation [83]), future work should study how such prior experience influences users' disclosure behavior.

7. Conclusion

Many users discontinue the disclosure of their PHI after some time, thereby foregoing potential health benefits. Drawing on a configurational perspective of privacy calculus theory that accounts for the evolving perceptions of users over time, we identified four configurations of users' expected and experienced benefits and costs that explain users' discontinuous disclosure intention. We introduce discontinuous disclosure as a new disclosure behavior and extend privacy calculus theory to account for how expected and experienced benefits and costs work together to explain users' discontinuous disclosure.

CRediT authorship contribution statement

Florian Wintmölle: Writing – original draft, Writing – review & editing, Conceptualization, Methodology, Investigation, Data curation, Formal analysis, Software, Visualization, Validation, Project administration. **Marco Meier:** Writing – review & editing, Conceptualization, Methodology, Investigation. **Christian Maier:** Writing – review & editing, Conceptualization, Funding acquisition, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Privacy calculus theory in previous research

Privacy is by nature context-sensitive [84] because the type of information to be disclosed varies, meaning that the importance of certain benefits and costs differs depending on the specific context. For instance, personal information regarded as more sensitive by the user, such as financial data, increases risk beliefs and decreases the intention to disclose such information [26]. In line with this, users' tradeoffs tend to be context-specific, displaying substantial heterogeneity in the factors considered across different contexts. For example, while crucial benefits of location-based services include the ability to determine an individual's physical location, known as locatability, and personalization [13], informational and emotional support are important benefits for online health communities [9]. Both contexts involve privacy risks as costs stemming from the disclosure of personal information [9,13], yet their intensity varies due to the context-sensitivity and information involved [26]. This means that, whereas the cost side primarily depends on the information sensitivity and tends to be rather consistent with respect to the costs considered, there is less consistency on the benefit side because the benefits are more context-specific, implying that different benefits are relevant in different contexts. Given this inherent context-sensitivity and context specificity of benefits and costs and their relationship to disclosure behavior, prior IS research has established a body of literature on privacy calculus theory across numerous contexts, weighing various benefits and costs.

In Table A1, we summarize representative research drawing on privacy calculus theory. We gathered IS literature from the senior scholars' list of premier journals[1] using the Web of Science Database and the search string ("privacy calculus" OR "privacy paradox" OR "privacy tradeoff" OR "privacy concern" OR "risk calculus" OR "privacy decision-making" OR "privacy attitudes"). We included all studies using a privacy tradeoff to examine individuals' disclosure behavior in different contexts, assessing different benefits, costs, and outcomes.

Table A1
Representative research on privacy calculus theory.

Reference	Context	Benefits	Costs	Outcome
[14]	Location-aware marketing	Perceived benefit of information disclosure	Perceived risk of information disclosure	Willingness to have personal information used in LAM
[43]	Mobile app	Perceived app value	App intrusiveness, privacy concerns	Permission acceptance intention

(continued on next page)

[1] https://aisnet.org/page/SeniorScholarListofPremierJournals

Table A1 (*continued*)

Reference	Context	Benefits	Costs	Outcome
[15]	Social network application	Perceived benefit (Social rewards, enjoyment, ubiquity, timeliness)	Privacy concern	Initial use/Continued Use, Self-disclosure
[45]	Mobile app (driving behavior app for insurance firms)	Perceived benefits of information disclosure	Perceived risks of information disclosure	Intention to disclose
[13]	Location-based service	Perceived benefits of information disclosure (Locatability, personalization)	Perceived risks of information disclosure	Intention to disclose personal information in LBS
[24]	Synchronous online social interaction (Online chat room)	Social rewards	Privacy concerns	Self-disclosure, misrepresentation
[85]	Unfamiliar online vendor	Privacy protection belief	Privacy risk belief	Behavioral intention
[7]	E-commerce transaction	Internet trust	Internet privacy concerns	Willingness to provide personal information to transact on the Internet
[11]	IT-enabled ride-sharing	Perceived benefits of information privacy disclosure	Perceived risks of information privacy disclosure	Intention to disclose information, disclosure of personal information
[86]	E-commerce	Benefits of disclosing information	Costs of disclosing information	Information disclosure, coupon redemption
[48]	Social networking site	Perceived Benefits (Self-expression, life documentation, social rewards)	Privacy risks	Intention to disclose
[46]	Social app	Social rewards, personalized benefits	Privacy concerns	Misrepresentation behavior
[87]	E-commerce	Tangible benefits (e.g., discount), intangible benefits (e.g., personalization accuracy)	Tangible costs (e.g., spam mails), intangible costs (e.g., risk of personal information being traded)	Willingness to disclose personal data
[8]	Online social network	Socialization, self-expression, pleasing others, information seeking	Disclosure of (or relinquishment of control over) information	Information and interaction management behaviors
[88]	Online social connectivity management	Expected social capital gains	Privacy risks	No action, acceptance
[49]	Virtual health community	Expected positive personal outcomes of sharing PHI, expected positive community-related outcomes of sharing PHI	PHI privacy concern	Willingness to communicate PHI
[25]	Standalone personal health record system	Perceived benefit	Perceived privacy risk	Intention to use standalone PHR
[89]	Mobile app (Location-based service)	Perceived benefit	Perceived risk	Disclosure
[23]	Healthcare	Trust in electronic medium	Electronic health information privacy concern	Willingness to provide access to personal health information
[9]	Online health community	Informational support, emotional support	Health information privacy concerns	PHI disclosure intention
[90]	Sharing economy	Economic benefit	Privacy concerns	Intention to share
[91]	E-commerce	Perceived need for government surveillance	Government intrusion concerns, internet privacy concerns	Willingness to provide personal information to transact on the internet
[92]	Online social network	Convenience of maintaining relationships, relationship building, self-presentation, enjoyment	Perceived privacy risk	Privacy-related behavior (e.g., information disclosure/ falsification)
[39]	E-commerce	Institutional trust	Privacy concerns	E-commerce use
[93]	Check-in service (Location-based service)	Conditional value (Location, time, identity)	Privacy risk	Disclosure intention
[94]	Controversial information technologies	Account security, convenience	Privacy concerns, security concerns	Attitude

Appendix B. Participant exclusion and demographics

In total, 755 participants passed the screening survey, of which 571 participants took part in the main study. We removed 66 participants who did not finish the survey and 165 additional participants who provided contradictory responses in the screening survey compared to the follow-up survey. We excluded 18 participants because they omitted more than two items, had a standard deviation below 0.5 across their responses, indicating inaccurate responses [95], or responded in less than three minutes, which is unrealistically quick given that the average survey completion time was more than eight minutes, with a standard deviation of four minutes [73]. We present the demographic characteristics of our final sample consisting of 322 users in Table B1.

Table B1
Demographics of the survey participants.

Age (%)		Sex (%)		Education (%)		App (%)	
<25	22.98	Male	45.65	Less than high school	0.62	Apple Health	36.96
25–34	37.27	Female	54.04	High school	14.29	Google Fit	17.08
35–44	18.32	Missing	0.31	Some college	22.98	Fitbit	10.87
45–54	11.49			Bachelor’s degree	42.55	MyFitnessPal	20.19
>54	9.32			Master’s degree	16.15	Other	14.91
Missing	0.62			Doctoral degree	3.42		

Appendix C. Measures considered in the privacy calculi

Table C1
Benefits and costs considered in users' tradeoffs of expectations and experiences.

Construct	Item	Loading
Expected health benefits (adapted from [25])	I expected disclosing my personal health information to {APP} would improve my ability to manage my health.	0.87
	I expected disclosing my personal health information to {APP} would improve the quality of my health management.	0.89
	I expected I would manage my health more effectively when disclosing my personal health information to {APP}.	0.82
Expected personalization (adapted from [13])	I expected {APP} to provide me with personalized services tailored to my health management.	0.80
	I expected {APP} to provide me with more relevant health information tailored to my personal preferences or personal interests.	0.88
	I expected {APP} to provide me with the kind of health information or service that I might like.	0.76
Expected trust (adapted from [26])	I trusted that {APP} would keep my best interests in mind when dealing with personal health information.	0.88
	I expected {APP} to be generally predictable and consistent regarding the usage of personal health information.	0.86
	I expected {APP} to be always honest with users when it comes to using personal health information that I would provide.	0.87
Expected privacy concerns (adapted from [39])	I was concerned that the personal health information I submit to {APP} could be misused.	0.89
	I was concerned that a person could access my personal health information through {APP}.	0.90
	I was concerned about submitting personal health information to {APP}, because of what others might do with it.	0.93
	I was concerned about submitting personal health information to {APP}, because it could be used in a way I did not foresee.	0.92
Experienced health benefits (adapted from [25])	Disclosing my personal health information to {APP} improves my ability to manage my health.	0.87
	Disclosing my personal health information to {APP} improves the quality of my health management.	0.92
	I manage my health more effectively due to the disclosure of my personal health information to {APP}.	0.85
Experienced personalization (adapted from [13])	{APP} can provide me with personalized services tailored to my health management.	0.87
	{APP} can provide me with more relevant health information tailored to my preferences or personal interests.	0.90
	{APP} can provide me with the kind of health information or service that I might like.	0.81
Experienced trust (adapted from [26])	I trust that {APP} keeps my best interests in mind when dealing with personal health information.	0.84
	{APP} is generally predictable and consistent regarding the usage of my personal health information.	0.83
	{APP} is always honest with users when it comes to using personal health information that I would provide.	0.85
Experienced privacy concerns (adapted from [39])	I am concerned that the personal health information I submit to {APP} is being misused.	0.93
	I am concerned that a person can access my personal health information through {APP}.	0.94
	I am concerned about submitting personal health information to {APP}, because of what others do with it.	0.97
	I am concerned about submitting personal health information to {APP}, because it is being used in a way I did not foresee.	0.93
Discontinuous disclosure intention (adapted from [9])	I am likely to stop revealing my personal health information in {APP}.	0.98
	It is probable that I will stop revealing my personal health information in {APP}.	0.97
	I will stop revealing my personal health information in {APP}.	0.96

Appendix D. Descriptive statistics and measurement validation

We checked for common method bias (CMB) using Harman's single-factor test. This test assesses the extent to which a single factor can explain the variance in the data [60]. The test revealed that only 37.72 % of the variance is explained by one factor, which is considerably below the recommended threshold of 50 %. Moreover, we examined the correlation matrix for very high correlations ($r > 0.90$) [96] (see Table D1). Both tests indicate that CMB is not an issue. According to QCA recommendations, it is advisable to maintain a conditions-to-observations ratio of less than 0.20 [97]. Since we examined eight conditions with 322 observations, the ratio is 0.02, indicating that the sample size is appropriate.

Table D1
Descriptive statistics and discriminant validity.

	Construct	M	SD	α	CR	AVE	1	2	3	4	5	6	7	8	9
1	Expected health benefits	5.78	0.92	0.89	0.89	0.74	**0.86**								
2	Expected personalization	5.47	1.07	0.85	0.86	0.67	0.44	**0.82**							
3	Expected trust	5.49	1.12	0.90	0.90	0.76	0.45	0.33	**0.87**						
4	Expected privacy concerns	4.06	1.65	0.95	0.95	0.83	−0.17	0.09	−0.31	**0.91**					
5	Experienced health benefits	5.12	1.20	0.91	0.91	0.77	0.42	0.22	0.31	−0.21	**0.88**				
6	Experienced personalization	4.98	1.17	0.89	0.90	0.74	0.31	0.38	0.25	−0.12	0.65	**0.86**			
7	Experienced trust	4.84	1.24	0.88	0.88	0.71	0.29	0.12	0.58	−0.38	0.56	0.47	**0.84**		
8	Experienced privacy concerns	3.92	1.71	0.97	0.97	0.89	−0.17	0.18	−0.24	0.71	−0.30	−0.12	−0.48	**0.94**	
9	Discontinuous disclosure intention	3.82	1.94	0.98	0.98	0.94	−0.13	0.10	−0.23	0.43	−0.51	−0.32	−0.49	0.50	**0.97**

Note: square root of AVE is listed on the diagonal of bivariate correlations; M = Mean; SD = standard deviation; AVE = average variance extracted; CR = composite reliability; α = Cronbach's alpha.

Appendix E. Two-step fsQCA

Given fsQCA's set-theoretical nature, the conditions and the outcome must be calibrated into fuzzy set memberships, ranging from zero to one. We employed direct calibration using three membership anchors [68], which is suited for data measured on Likert scales [62,74]. Therefore, we calculated the mean for each condition and set the three anchors based on the seven-point Likert scale: the minimum value of one for full non-membership, the mean value of four for the crossover point, and the maximum value of seven for full membership. A resulting fuzzy value of zero indicates full non-membership, while a resulting fuzzy value of one indicates full membership. For instance, a fuzzy value of zero for discontinuous disclosure intention indicates a low discontinuous disclosure intention of PHI, whereas a fuzzy value of one indicates a high discontinuous disclosure intention. To avoid fuzzy values of 0.50, which are excluded by the fsQCA algorithm, we followed the methodology described in previous studies and added a small constant of 0.001 [74]. Because all constructs use the same scale, this calibration applies equally to the conditions and the outcome.

The first step of the two-step fsQCA consists of an analysis of necessity to analyze remote conditions [17]. Essentially, it aims to identify combinations of necessary expected conditions (i.e., the combination of expected health benefits, expected personalization, expected trust, and expected privacy concerns) that enable discontinuous disclosure intention. These combinations consist of expressions composed of disjunctions, representing a logical OR, or conjunctions, representing a logical AND, or they consist of expressions composed of both disjunctions and conjunctions [71]. This means that disjunctions, conjunctions, or combinations of them together may form a consistent necessary context for the outcome. Consistency thereby describes the extent to which observations exhibiting a particular solution also display the outcome [72]. A solution refers to a specific combination of conditions that leads to a particular outcome [68]. To ensure that a significant portion of observations exhibiting the solution are included within the subset of observations that exhibit the outcome, it is recommended to employ a high consistency threshold of 0.90 [69]. Not all identified consistent contexts can automatically be considered reasonable contexts necessary for the outcome. They must also meet the criteria of empirical relevance [17]. This means that a necessary context must also pass a coverage threshold of 0.60 [72] and a relevance of necessity threshold of 0.50 to be necessary [17]. Additionally, researchers need to establish theoretical soundness of the context by being able to name it, because otherwise, no reasonable assertion of necessity of the context is possible [17].

The second step of the two-step fsQCA consists of an analysis of sufficiency, which reveals remote-proximate conjunctions. So, the identified necessary context from the first step is considered together with the proximate conditions [17]. This means that in addition to the expected benefits and costs identified as necessary in step 1, all experienced benefits and costs are analyzed together. Because Step 1 might identify conjunctions, disjunctions, or a combination of both as necessary context, it is important to note that within the set-theoretic framework, all underlying conditions are themselves implicitly necessary [71]. This allows Step 2 of the analysis to include the remote conditions themselves rather than the necessary context as a whole.

For the analysis of the sufficient configurations, we created a truth table including all logically possible configurations of necessary remote conditions and proximate conditions. The truth table included 2^k possible configurations, with k representing the number of conditions (i.e., the identified necessary remote conditions from Step 1 and all proximate conditions). We reduced the truth table by using a frequency threshold of four, which is established in QCA studies [98,99], and suited for larger sample sizes [100]. After dropping configurations with fewer observations, 93.17 % of the observations in the sample remained, which is in line with recommendations suggesting that the frequency threshold should preserve at least 80 % of the observations in the analysis [101]. We used a consistency threshold of 0.80 [17], which contributes to reliable results [68]. We simplified the remaining truth table using the Quine-McCluskey algorithm, which logically minimizes the solution [68]. Using the conservative solution, we empirically capture the causal complex relationship between the expected and experienced benefits and costs and discontinuous disclosure intention in a non-parsimonious manner. When employing this algorithm, “don’t care” situations may arise, signifying that a condition in a particular sufficient configuration can be either high or low, making it irrelevant for discontinuous disclosure intention. We provide the resulting truth table of the fsQCA in Table E1.

Table E1
Truth table for discontinuous disclosure intention.

POT	POP	POH	POC	PRH	PRP	DID	Number	Raw consistency	PRI
0	0	0	1	1	1	1	9	0.92	0.75
1	0	0	1	1	1	1	7	0.92	0.70
0	1	0	1	1	1	1	9	0.91	0.72
1	1	0	1	1	1	1	4	0.90	0.65
1	0	0	0	1	1	1	4	0.88	0.56
1	0	1	1	1	1	1	5	0.87	0.58
1	1	0	0	1	1	1	4	0.87	0.53
0	1	1	1	1	1	1	22	0.86	0.63
1	0	1	0	1	0	0	4	0.79	0.25
1	1	0	1	1	0	0	6	0.78	0.37
1	1	1	1	1	1	0	108	0.78	0.53
1	1	1	0	1	0	0	9	0.75	0.25
1	1	1	0	1	1	0	109	0.58	0.24

Note: ’POT’ indicates experienced trust, ’POP’ indicates experienced personalization, ’POH’ indicates experienced health benefits, ’POC’ indicates experienced privacy concerns, ’PRH’ indicates expected health benefits, ’PRP’ indicates expected personalization, ’DID’ indicates discontinuous disclosure intention.

In addition to identifying configurations that lead to discontinuous disclosure intention, we further conducted an fsQCA for the absence of such intention, following the same guidelines. Similarly, the fsQCA therefore first involved a necessity analysis of the remote conditions. Under the same thresholds as for discontinuous disclosure intention (consistency > 0.9, coverage > 0.6, relevance of necessity > 0.5), no necessary conditions were identified. Subsequently, we performed the sufficiency analysis and revealed one sufficient configuration for the absence of discontinuous disclosure intention (solution coverage $= 0.75$, solution consistency $= 0.84$). This configuration highlights a pathway where users do not develop an intention to discontinue disclosure when they experience trust but no privacy concerns. It is important to note that the absence of discontinuous disclosure intention is not necessarily synonymous with active continuous disclosure. Rather, it indicates a state where the factors for discontinuing disclosure are not simply present. This is because fsQCA allows for causal asymmetry, meaning the conditions sufficient for an outcome can differ from those sufficient for its absence [62]. We provide a graphical representation in Table E2 and the truth table in Table E3.

Table E2
Configurations for absence of discontinuous disclosure intention.

Tradeoff of expectations	Expected health benefits	
	Expected personalization	
	Expected trust	
	Expected privacy concerns	
Tradeoff of experiences	Experienced health benefits	
	Experienced personalization	
	Experienced trust	●
	Experienced privacy concerns	⊗
	Raw coverage	0.75
	Unique coverage	0.75
	Consistency	0.84
	Solution coverage	0.75
	Solution consistency	0.84

Note: Black circles (●) indicate the presence of a condition, white crossed-out circles (⊗) indicate the absence of a condition, and blank spaces () indicate "don't care" situations. In these cases, the specific conditions are irrelevant to the configuration and can be present or absent.

Table E3
Truth table for no discontinuous disclosure intention.

POT	POP	POH	POC	~DID	Number	Raw consistency	PRI
1	0	1	0	1	10	0.88	0.65
1	1	1	0	1	119	0.86	0.76
1	1	0	0	1	5	0.85	0.49
1	0	0	0	1	7	0.85	0.45
1	0	1	1	0	5	0.82	0.42
1	1	0	1	0	5	0.81	0.36
1	0	0	1	0	7	0.80	0.30
0	1	0	1	0	12	0.77	0.28
0	1	1	1	0	24	0.77	0.38
0	0	0	1	0	11	0.75	0.24
1	1	1	1	0	112	0.74	0.44

Note: 'POT' indicates experienced trust, 'POP' indicates experienced personalization, 'POH' indicates experienced health benefits, 'POC' indicates experienced privacy concerns, '~DID' indicates absence of discontinuous disclosure intention.

Appendix F. Robustness of the results

To ensure the validity of our identified solutions for discontinuous disclosure intention, we conducted several sensitivity analyses [62,102], testing the robustness of the solutions to variations in the key analytical parameters. These analyses included sensitivity tests for the consistency threshold, the frequency threshold, and the calibration anchors. For each test, we identified the ranges within which our solutions remained stable. Detailed results of these sensitivity analyses are summarized in Table F1. Regarding sensitivity to the consistency threshold, the analysis revealed that the solution remained stable within a range of 0.80 to 0.84, indicating that the solution is not overly sensitive to minor changes in this parameter. Regarding sensitivity to the frequency threshold, the analysis revealed that the solution remained stable only at the threshold of four. To further assess this sensitivity to the sample, we manually lowered the frequency threshold to three, thereby excluding combinations with fewer than three observations. Repeated analyses with the decreased threshold showed substantially the same results with only minimal deviations, indicating overall robustness of the solutions even with a slightly less strict frequency threshold. Regarding sensitivity to the calibration anchors, the analysis revealed that the solution remained stable for the full-membership anchor (initial threshold 7) with a lower bound of 4 and without an identifiable upper bound within the empirically tested range. This indicates very high robustness, as the solution remained identical even when the threshold was iteratively increased beyond the highest value observed in the raw data [102]. The crossover anchor (initial threshold 4) demonstrated stability between 3.6 and 4.7, and the full-non-membership anchor (initial threshold 1) remained unchanged within the range of 0.8 to 1.5. In sum, the sensitivity analyses collectively highlight our solution's overall robustness, indicating its stability across changes in consistency thresholds, frequency thresholds, and calibration anchors.

Table F1
Sensitivity analysis for discontinuous disclosure intention.

		Lower bound	Threshold	Upper bound
Consistency		0.8	0.8	0.86
Frequency		4	4	4
Calibration	Full membership	4	7	> 7
	Crossover	3.6	4	4.7
	Full non-membership	0.8	1	1.5

Moreover, to empirically validate whether our sequential, two-step research model is meaningful and appropriate, we conducted an alternative one-step fsQCA as a robustness check. The purpose of this analysis was to test whether this flat one-step model, which does not distinguish between temporally and causally distant user expectations and proximate user experiences, could adequately explain discontinuous disclosure. Accordingly, all eight proximate and remote conditions (i.e., expected and experienced health benefits, personalization, trust, and privacy concerns) were included simultaneously in the analysis. Following recent IS research [103], we set a frequency threshold of three to ensure empirical relevance [73], a raw consistency threshold of 0.85 to identify reliably sufficient conditions [72,103], and a Proportional Reduction in Inconsistency (PRI) threshold of 0.75 to avoid solutions that predict both a high and a low outcome and thus yield contradictory configurations [104]. We performed the sufficiency analysis by first creating a truth table containing all logically possible combinations of the eight conditions and then applying the minimization algorithm to this table. The analysis revealed that no configuration within the truth table met all thresholds. Consequently, the algorithm could not produce a solution, resulting in an "empty solution." For full transparency, we present the truth table of all empirically relevant configurations, all of which were consequently coded with an outcome value of "0," in Table F2. This null result provides strong empirical support for our theoretical argument that a non-sequential model is insufficient to capture the complexity of discontinuous disclosure. It underscores the necessity of the two-step approach, which distinguishes between the baseline of user expectations and their subsequent evaluation of experiences, to provide a meaningful and robust explanation for the observed behavior. Therefore, the choice of the two-step fsQCA is not only theoretically justified but also validated by this empirical robustness check.

Table F2
Truth table for discontinuous disclosure intention.

PRT	PRH	PRP	PRC	POT	POH	POP	POC	DID	Number	Raw consistency	PRI
1	1	1	1	0	0	0	1	0	5	0.92	0.73
1	1	1	0	0	0	0	1	0	3	0.92	0.67
1	1	1	1	1	0	0	1	0	6	0.92	0.69
1	1	1	1	0	0	1	1	0	5	0.91	0.70
1	1	1	1	1	0	1	1	0	4	0.90	0.64
1	1	1	1	1	0	1	0	0	3	0.89	0.57
1	1	1	1	1	1	0	1	0	4	0.87	0.58
1	1	1	0	0	1	1	1	0	4	0.87	0.55
0	1	1	1	0	1	1	1	0	7	0.87	0.54
1	1	1	1	0	1	1	1	0	11	0.87	0.61
1	1	0	0	1	0	0	0	0	3	0.86	0.34
1	1	1	0	1	1	1	1	0	19	0.81	0.45
1	1	1	1	1	1	1	1	0	88	0.80	0.55
1	1	0	0	1	1	0	0	0	3	0.79	0.21
1	1	1	0	1	1	0	0	0	3	0.78	0.33
1	1	1	1	1	1	1	0	0	23	0.77	0.37
1	1	0	0	1	1	1	0	0	9	0.75	0.21
1	1	1	0	1	1	1	0	0	85	0.58	0.22

Note: 'PRT' indicates expected trust, 'PRH' indicates expected health benefits, 'PRP' indicates expected personalization, 'PRC' indicates expected privacy concerns, 'POT' indicates experienced trust, 'POH' indicates experienced health benefits, 'POP' indicates experienced personalization, 'POC' indicates experienced privacy concerns, 'DID' indicates discontinuous disclosure intention.

References

[1] F. Garamvolgyi, Why US Women Are Deleting Their Period Tracking Apps, The Guardian, 2022. https://www.theguardian.com/world/2022/jun/28/why-us-woman-are-deleting-their-period-tracking-apps. accessed June 26, 2024.

[2] S. McCallum, T. Singleton, Period Trackers "Coercing" Women into Sharing Risky Information, BBC, 2024. https://www.bbc.com/news/articles/cmj6j3d8xjjo. accessed June 26, 2024.

[3] R. Stropute, Kilo Health Digital Health and Wellness Report 2022, Kilo Health, 2022. https://news.cision.com/kilo-health/r/doing-my-own-research–why-don-t-americans-use-health-apps-but-follow-the-advice-they-find-online-,c3650061.

[4] M. Hong, V. Rajaguru, K. Kim, S.-Y. Jang, S.G. Lee, Menstrual cycle management and period tracker app use in millennial and generation Z individuals: mixed methods study, J. Med. Internet. Res. 26 (2024) e53146, https://doi.org/10.2196/53146.

[5] C. Mack, Y. Terhorst, M. Stephan, H. Baumeister, M. Stach, E.-M. Messner, J. Bengel, L.B. Sander, Help in a heartbeat?": a systematic evaluation of mobile health applications (apps) for coronary heart disease, Int. J. Environ. Res. Public Health 18 (2021) 10323, https://doi.org/10.3390/ijerph181910323.

[6] P. Menard, G.J. Bott, Artificial intelligence misuse and concern for information privacy: new construct validation and future directions, Inf. Syst. J. 35 (2024) 322–367, https://doi.org/10.1111/isj.12544.

[7] T. Dinev, P. Hart, An extended privacy calculus model for e-commerce transactions, Inf. Syst. Res. 17 (2006) 61–80, https://doi.org/10.1287/isre.1060.0080.

[8] T.L. James, M. Warkentin, S.E. Collignon, A dual privacy decision model for online social networks, Inf. Manag. 52 (2015) 893–908, https://doi.org/10.1016/j.im.2015.07.010.

[9] X. Zhang, S. Liu, X. Chen, L. Wang, B. Gao, Q. Zhu, Health information privacy concerns, antecedents, and information disclosure intention in online health communities, Inf. Manag. 55 (2018) 482–493, https://doi.org/10.1016/j.im.2017.11.003.

[10] M.J. Culnan, R.J. Bies, Consumer privacy: balancing economic and justice considerations, J. Soc. Issues 59 (2003) 323–342, https://doi.org/10.1111/1540-4560.00067.

[11] X. Cheng, T. Hou, J. Mou, Investigating perceived risks and benefits of information privacy disclosure in IT-enabled ride-sharing, Inf. Manag. 58 (2021) 103450, https://doi.org/10.1016/j.im.2021.103450.

[12] C.L. Miltgen, H.J. Smith, Falsifying and withholding: exploring individuals' contextual privacy-related decision-making, Inf. Manag. 56 (2019) 696–717, https://doi.org/10.1016/j.im.2018.11.004.

[13] H. Xu, H.-H. Teo, B.C.Y. Tan, R. Agarwal, The role of push-pull technology in privacy calculus: the case of location-based services, J. Manag. Inf. Syst. 26 (2009) 135–174, https://doi.org/10.2753/MIS0742-1222260305.

[14] H. Xu, X. Luo, J.M. Carroll, M.B. Rosson, The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing, Decis. Support Syst. 51 (2011) 42–52, https://doi.org/10.1016/j.dss.2010.11.017.

[15] M. Koohikamali, A.M. French, D.J. Kim, An investigation of a dynamic model of privacy trade-off in use of mobile social network applications: a longitudinal perspective, Decis. Support Syst. 119 (2019) 46–59, https://doi.org/10.1016/j.dss.2019.02.007.

[16] A. Acquisti, C. Taylor, L. Wagman, The economics of privacy, J. Econ. Lit. 54 (2016) 442–492, https://doi.org/10.1257/jel.54.2.442.

[17] C.Q. Schneider, Two-step QCA revisited: the necessity of context conditions, Qual. Quant. 53 (2019) 1109–1126, https://doi.org/10.1007/s11135-018-0805-7.

[18] E. Davidson, J.S. Winter, M. Chiasson, IT-based regulation of personal health: nudging, mobile apps and data, J. Inf. Technol. 38 (2023) 108–125, https://doi.org/10.1177/02683962221112678.

[19] S.R. Steinhubl, E.D. Muse, E.J. Topol, The emerging field of mobile health, Sci. Transl. Med. 7 (2015), https://doi.org/10.1126/scitranslmed.aaa3487.

[20] C. Kao, D.M. Liebovitz, Consumer mobile health apps: current state, barriers, and future directions, PM&R 9 (2017), https://doi.org/10.1016/j.pmrj.2017.02.018.

[21] B. Ramsey, What are mHealth Apps? Types, Examples, Costs, and More, Scopic (2024). https://scopicsoftware.com/blog/mobile-health-apps/(accessed November 20, 2024).

[22] V. Vijayan, J.P. Connolly, J. Condell, N. McKelvey, P. Gardiner, Review of wearable devices and data collection considerations for connected health, Sensors 21 (2021) 5589, https://doi.org/10.3390/s21165589.

[23] C.L. Anderson, R. Agarwal, The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information, Inf. Syst. Res. 22 (2011) 469–490, https://doi.org/10.1287/isre.1100.0335.

[24] Z. Jiang, C.S. Heng, B.C.F. Choi, Research note - privacy concerns and privacy-protective behavior in synchronous online social interactions, Inf. Syst. Res. 24 (2013) 579–595, https://doi.org/10.1287/isre.1120.0441.

[25] H. Li, A. Gupta, J. Zhang, R. Sarathy, Examining the decision to use standalone personal health record systems as a trust-enabled fair social contract, Decis. Support Syst. 57 (2014) 376–386, https://doi.org/10.1016/j.dss.2012.10.043.

[26] N.K. Malhotra, S.S. Kim, J. Agarwal, Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model, Inf. Syst. Res. 15 (2004) 336–355, https://doi.org/10.1287/isre.1040.0032.

[27] L. Chen, A. Baird, A. Rai, Mobile health (mHealth) channel preference: an integrated perspective of approach - avoidance beliefs and regulatory focus, J. Assoc. Inf. Syst. 20 (2019) 1743–1773, https://doi.org/10.17705/1jais.00584.

[28] M. Han, E. Lee, Effectiveness of mobile health application use to improve health behavior changes: a systematic review of randomized controlled trials, Healthc. Inform. Res. 24 (2018) 207, https://doi.org/10.4258/hir.2018.24.3.207.

[29] N.F. Awad, M.S. Krishnan, The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization, MIS Q. 30 (2006) 13. 10.2307/25148715.

[30] R.K. Chellappa, S. Shivendu, An economic model of privacy: a property rights approach to regulatory choices for online personalization, J. Manag. Inf. Syst. 24 (2007) 193–225, https://doi.org/10.2753/MIS0742-1222240307.

[31] T.-P. Liang, H.-J. Lai, Y.-C. Ku, Personalized content recommendation and user satisfaction: theoretical synthesis and empirical findings, J. Manag. Inf. Syst. 23 (2006) 45–70, https://doi.org/10.2753/MIS0742-1222230303.

[32] J. Sutanto, E. Palme, C.-H. Tan, C.W. Phang, Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users, MIS Q. 37 (2013) 1141–1164, https://doi.org/10.25300/MISQ/2013/37.4.07.

[33] S.E. Short, S. Mollborn, Social determinants and health behaviors: conceptual frames and empirical advances, Curr. Opin. Psychol. 5 (2015) 78–84, https://doi.org/10.1016/j.copsyc.2015.05.002.

[34] X. Guo, X. Zhang, Y. Sun, The privacy–personalization paradox in mHealth services acceptance of different age groups, Electron. Commer. Res. Appl. 16 (2016) 55–65, https://doi.org/10.1016/j.elerap.2015.11.001.

[35] F. Monteiro-Guerra, O. Rivera-Romero, L. Fernandez-Luque, B. Caulfield, Personalization in real-time physical activity coaching using mobile applications: a scoping review, IEEE J. Biomed. Health Inform. 24 (2020) 1738–1751, https://doi.org/10.1109/JBHI.2019.2947243.

[36] P. Tarafdar, I. Bose, Recognition of human activities for wellness management using a smartphone and a smartwatch: a boosting approach, Decis. Support Syst. 140 (2021) 113426, https://doi.org/10.1016/j.dss.2020.113426.

[37] U. Varshney, A model for improving quality of decisions in mobile health, Decis. Support Syst. 62 (2014) 66–77, https://doi.org/10.1016/j.dss.2014.03.005.

[38] K. Anderson, O. Burford, L. Emmerton, Mobile health apps to facilitate self-care: a qualitative study of user experiences, PLoS One 11 (2016) e0156164, https://doi.org/10.1371/journal.pone.0156164.

[39] T. Dinev, M. Bellotto, P. Hart, V. Russo, I. Serra, C. Colautti, Privacy calculus model in e-commerce – a study of Italy and the United States, Eur. J. Inf. Syst. 15 (2006) 389–402, https://doi.org/10.1057/palgrave.ejis.3000590.

[40] S. Ganesan, Determinants of long-term orientation in buyer-seller relationships, J. Mark. 58 (1994) 1–19, https://doi.org/10.1177/002224299405800201.

[41] J.F. Yates, E.R. Stone, The risk construct. Risk Taking Behavior, John Wiley & Sons, 1992, pp. 1–26.

[42] R.S. Laufer, M. Wolfe, Privacy as a concept and a social issue: a multidimensional developmental theory, J. Soc. Issues 33 (1977) 22–42, https://doi.org/10.1111/j.1540-4560.1977.tb01880.x.

[43] V.M. Wottrich, E.A. van Reijmersdal, E.G. Smit, The privacy trade-off for mobile app downloads: the roles of app value, intrusiveness, and privacy concerns, Decis. Support Syst. 106 (2018) 44–52, https://doi.org/10.1016/j.dss.2017.12.003.

[44] T. Dinev, H. Xu, J.H. Smith, P. Hart, Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts, Eur. J. Inf. Syst. 22 (2013) 295–316, https://doi.org/10.1057/ejis.2012.23.

[45] F. Kehr, T. Kowatsch, D. Wentzel, E. Fleisch, Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus: privacy calculus: dispositions and affect, Inf. Syst. J. 25 (2015) 607–635, https://doi.org/10.1111/isj.12062.

[46] Y. Tang, X. Ning, Understanding user misrepresentation behavior on social apps: the perspective of privacy calculus theory, Decis. Support Syst. 165 (2023) 113881, https://doi.org/10.1016/j.dss.2022.113881.

[47] G. Fox, R. Connolly, Mobile health technology adoption across generations: narrowing the digital divide, Inf. Syst. J. 28 (2018) 995–1019, https://doi.org/10.1111/isj.12179.

[48] Y. Sun, N. Wang, X.-L. Shen, Calculus interdependency, personality contingency, and causal asymmetry: toward a configurational privacy calculus model of information disclosure, Inf. Manag. 58 (2021) 103556, https://doi.org/10.1016/j.im.2021.103556.

[49] N. Kordzadeh, J. Warren, Communicating personal health information in virtual health communities: an integration of privacy calculus model and affective commitment, J. Assoc. Inf. Syst. 18 (2017) 45–81, https://doi.org/10.17705/1jais.00446.

[50] H.J. Smith, S.J. Milberg, S.J. Burke, Information privacy: measuring individuals' concerns about organizational practices, MIS Q. 20 (1996) 167–196, https://doi.org/10.2307/249477.

[51] J. Recker, Reasoning about discontinuance of information system use, J. Inf. Technol. Theory Appl. 17 (2016) 41–66.

[52] A. Acquisti, L. Brandimarte, G. Loewenstein, Privacy and human behavior in the age of information, Science (1979) 347 (2015) 509–514, https://doi.org/10.1126/science.aaa1465.

[53] F. Liu, E.T.K. Lim, H. Li, C.-W. Tan, D. Cyr, Disentangling utilitarian and hedonic consumption behavior in online shopping: an expectation disconfirmation perspective, Inf. Manag. 57 (2020) 103199, https://doi.org/10.1016/j.im.2019.103199.

[54] A. Bhattacherjee, Understanding information systems continuance: an expectation-confirmation model, MIS Q. 25 (2001) 351–370, https://doi.org/10.2307/3250921.

[55] R.L. Oliver, R.R. Burke, Expectation processes in satisfaction formation: a field study, J. Serv. Res. 1 (1999) 196–214, https://doi.org/10.1177/109467059913002.

[56] V. Santangelo, Forced to remember: when memory is biased by salient information, Behav. Brain Res. 283 (2015) 1–10, https://doi.org/10.1016/j.bbr.2015.01.013.

[57] K. Bauer, M. Von Zahn, O. Hinz, Expl(AI)ned: the impact of explainable artificial intelligence on users' information processing, Inf. Syst. Res. (2023), https://doi.org/10.1287/isre.2023.1199 isre.2023.1199.

[58] B.D. Douglas, P.J. Ewell, M. Brauer, Data quality in online human-subjects research: comparisons between MTurk, prolific, cloud research, qualtrics, and SONA, PLoS One 18 (2023) e0279720, https://doi.org/10.1371/journal.pone.0279720.

[59] E. Peer, D. Rothschild, A. Gordon, Z. Evernden, E. Damer, Data quality of platforms and panels for online behavioral research, Behav. Res. Methods 54 (2021) 1643–1662, https://doi.org/10.3758/s13428-021-01694-3.

[60] P.M. Podsakoff, S.B. MacKenzie, J.-Y. Lee, N.P. Podsakoff, Common method biases in behavioral research: a critical review of the literature and recommended remedies, J. Appl. Psychol. 88 (2003) 879–903, https://doi.org/10.1037/0021-9010.88.5.879.

[61] P. Sheeran, T.L. Webb, The intention–behavior gap, Soc. Personal. Psychol. Compass 10 (2016) 503–518, https://doi.org/10.1111/spc3.12265.

[62] J. Mattke, C. Maier, T. Weitzel, J.B. Thatcher, Qualitative comparative analysis in the information systems discipline: a literature review and methodological

recommendations, Internet Res. 31 (2021) 1493–1517, https://doi.org/10.1108/INTR-09-2020-0529.
[63] E. Carmines, R. Zeller, Reliability and Validity Assessment, SAGE Publications, Inc., 2008.
[64] C. Fornell, D.F. Larcker, Evaluating structural equation models with unobservable variables and measurement error, J. Mark. Res. 18 (1981) 39, https://doi.org/10.2307/3151312.
[65] D.T. Campbell, D.W. Fiske, Convergent and discriminant validation by the multitrait-multimethod matrix, Psychol. Bull. 56 (1959) 81–105, https://doi.org/10.1037/h0046016.
[66] J. Henseler, T.K. Dijkstra, M. Sarstedt, C.M. Ringle, A. Diamantopoulos, D. W. Straub, D.J. Ketchen, J.F. Hair, G.T.M. Hult, R.J. Calantone, Common beliefs and reality about PLS: comments on Rönkkö and Evermann (2013), Organ. Res. Methods 17 (2014) 182–209, https://doi.org/10.1177/1094428114526928.
[67] V.F. Misangyi, T. Greckhamer, S. Furnari, P.C. Fiss, D. Crilly, R. Aguilera, Embracing causal complexity: the emergence of a neo-configurational perspective, J. Manag. 43 (2017) 255–282, https://doi.org/10.1177/0149206316679252.
[68] C.C. Ragin, Redesigning Social Inquiry: Fuzzy Sets and Beyond, University of Chicago Press, 2008, https://doi.org/10.7208/chicago/9780226702797.001.0001.
[69] C.Q. Schneider, C. Wagemann, Set-Theoretic Methods for the Social Sciences: A Guide to Qualitative Comparative Analysis, 1st ed, Cambridge University Press, 2012, https://doi.org/10.1017/CBO9781139004244.
[70] C.Q. Schneider, C. Wagemann, Reducing complexity in Qualitative Comparative Analysis (QCA): remote and proximate factors and the consolidation of democracy, Eur. J. Polit. Res. 45 (2006) 751–786, https://doi.org/10.1111/j.1475-6765.2006.00635.x.
[71] A. Dușa, QCA With R, Springer International Publishing, Cham, 2019, https://doi.org/10.1007/978-3-319-75668-4.
[72] C.C. Ragin, Set relations in social research: evaluating their consistency and coverage, Polit. Anal. 14 (2006) 291–310, https://doi.org/10.1093/pan/mpj019.
[73] J. Mattke, C. Maier, L. Reis, T. Weitzel, Bitcoin investment: a mixed methods study of investment motivations, Eur. J. Inf. Syst. 30 (2021) 261–285, https://doi.org/10.1080/0960085X.2020.1787109.
[74] P.C. Fiss, Building better causal theories: a fuzzy set approach to typologies in organization research, Acad. Manag. J. 54 (2011) 393–420, https://doi.org/10.5465/amj.2011.60263120.
[75] P. Cichy, T.O. Salge, R. Kohli, Privacy concerns and data sharing in the internet of things: mixed methods evidence from connected cars, MIS Q. 45 (2021) 1863–1892, https://doi.org/10.25300/MISQ/2021/14165.
[76] M.J. Culnan, P.K. Armstrong, Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation, Organ. Sci. 10 (1999) 104–115, https://doi.org/10.1287/orsc.10.1.104.
[77] L. Festinger, A Theory of Cognitive Dissonance, Stanford University Press, 1957.
[78] G. Loomes, R. Sugden, Regret theory: an alternative theory of rational choice under uncertainty, Econ. J. 92 (1982) 805, https://doi.org/10.2307/2232669.
[79] M. Meier, C. Maier, J.B. Thatcher, T. Weitzel, Chatbot interactions: how consumption values and disruptive situations influence customers' willingness to interact, Inf. Syst. J. (2024) 12507, https://doi.org/10.1111/isj.12507 isj.
[80] F. Wintmölle, M. Meier, C. Maier, Artificial intelligence (AI) misuse: perpetrators' moral justifications, *ICIS 2024 Proceedings* (2024).
[81] K. Pflügner, C. Maier, J. Thatcher, J. Mattke, T. Weitzel, Deconstructing technostress: a configurational approach to explaining job burnout and job performance, MIS Q. 48 (2024) 679–698, https://doi.org/10.25300/MISQ/2023/16978.
[82] P. Sheeran, Intention—behavior relations: a conceptual and empirical review, Eur. Rev. Soc. Psychol. 12 (2002) 1–36, https://doi.org/10.1080/14792772143000003.
[83] A. Vance, J.L. Jenkins, B.B. Anderson, D.K. Bjornn, C.B. Kirwan, Tuning out security warnings: a longitudinal examination of habituation through fMRI, eye tracking, and field experiments, MIS Q. 42 (2018) 355–380, https://doi.org/10.25300/MISQ/2018/14124.
[84] S.T. Margulis, Privacy as a social issue and behavioral concept, J. Soc. Issues 59 (2003) 243–261, https://doi.org/10.1111/1540-4560.00063.
[85] H. Li, R. Sarathy, H. Xu, The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors, Decis. Support Syst. 51 (2011) 434–445, https://doi.org/10.1016/j.dss.2011.01.017.
[86] B. Koh, S. Raghunathan, B.R. Nault, An empirical examination of voluntary profiling: privacy and quid pro quo, Decis. Support Syst. 132 (2020) 113285, https://doi.org/10.1016/j.dss.2020.113285.
[87] H. Zhu, C.X.J. Ou, W.J.A.M. van den Heuvel, H. Liu, Privacy calculus and its utility for personalization services in e-commerce: an analysis of consumer decision-making, Inf. Manag. 54 (2017) 427–437, https://doi.org/10.1016/j.im.2016.10.001.
[88] B. Choi, Y. Wu, J. Yu, L. Land, Love at first sight: the interplay between privacy dispositions and privacy calculus in online social connectivity management, J. Assoc. Inf. Syst. 19 (2018) 124–151, https://doi.org/10.17705/1jais.00487.
[89] M.J. Keith, J.S. Babb, P.B. Lowry, C.P. Furner, A. Abdullat, The role of mobile-computing self-efficacy in consumer information disclosure: mobile-computing self-efficacy, Inf. Syst. J. 25 (2015) 637–667, https://doi.org/10.1111/isj.12082.
[90] T. Teubner, C.M. Flath, Privacy in the sharing economy, J. Assoc. Inf. Syst. 20 (2019) 213–242, https://doi.org/10.17705/1jais.00534.
[91] T. Dinev, P. Hart, M.R. Mullen, Internet privacy concerns and beliefs about government surveillance – an empirical investigation, J. Strateg. Inf. Syst. 17 (2008) 214–233, https://doi.org/10.1016/j.jsis.2007.09.002.
[92] H. Krasnova, S. Spiekermann, K. Koroleva, T. Hildebrand, Online social networks: why we disclose, J. Inf. Technol. 25 (2010) 109–125, https://doi.org/10.1057/jit.2010.6.
[93] T.-F. Kummer, S. Ryschka, M. Bick, Why do we share where we are? The influence of situational factors on the conditional value of check-in services, Decis. Support Syst. 115 (2018) 1–12, https://doi.org/10.1016/j.dss.2018.08.012.
[94] M. Breward, K. Hassanein, M. Head, Understanding consumers' attitudes toward controversial information technologies: a contextualization approach, Inf. Syst. Res. 28 (2017) 760–774, https://doi.org/10.1287/isre.2017.0706.
[95] A.J. Barends, R.E. de Vries, Noncompliant responding: comparing exclusion criteria in MTurk personality research to improve data quality, Personal. Individ. Differ. 143 (2019) 84–89, https://doi.org/10.1016/j.paid.2019.02.015.
[96] P. Pavlou, H. Liang, Y. Xue, Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective, MIS Q. 31 (2007) 105–136, https://doi.org/10.2307/25148783.
[97] A. Marx, Crisp-set qualitative comparative analysis (csQCA) and model specification: benchmarks for future csQCA applications, Int. J. Mult. Res. Approaches 4 (2010) 138–158, https://doi.org/10.5172/mra.2010.4.2.138.
[98] Q. Li, X. Zhang, W. Zhang, Organizational resilience and configurational conditions from the perspective of emergency: a fsQCA approach, Sage Open 13 (2023) 215824402311580, https://doi.org/10.1177/21582440231158057.
[99] G. Marzi, A. Marrucci, D. Vianelli, C. Ciappei, B2B digital platform adoption by SMEs and large firms: pathways and pitfalls, Ind. Mark. Manag. 114 (2023) 80–93, https://doi.org/10.1016/j.indmarman.2023.08.002.
[100] M. Maggetti, D. Levi-Faur, Dealing with errors in QCA, Polit. Res. Q. 66 (2013) 198–204, https://doi.org/10.1177/1065912912468269f.
[101] T. Greckhamer, V.F. Misangyi, P.C. Fiss, The two QCAs: from a small-N to a large-N set theoretic approach, in: P.C. Fiss, B. Cambré, A. Marx (Eds.), Research in the Sociology of Organizations, Emerald Group Publishing Limited, 2013, pp. 49–75, https://doi.org/10.1108/S0733-558X(2013)0000038007.
[102] I.-E. Oana, C.Q. Schneider, A robustness test protocol for applied QCA: theory and R software application, Sociol. Methods Res. 53 (2024) 57–88, https://doi.org/10.1177/00491241211036158.
[103] M. Meier, C. Maier, J.B. Thatcher, T. Weitzel, Cooking a telework theory with causal recipes: explaining telework success with ICT, work and family related stress, Inf. Syst. J. 34 (2023) 1068–1115, https://doi.org/10.1111/isj.12463.
[104] P.T. Leppänen, A.F. McKenny, J.C. Short, Qualitative comparative analysis in entrepreneurship: exploring the approach and noting opportunities for the future, in: B. Boyd, T.R. Crook, J.K. Lê, A.D. Smith (Eds.), Research Methodology in Strategy and Management, Emerald Publishing Limited, 2019, pp. 155–177, https://doi.org/10.1108/S1479-838720190000011010.

Florian Wintmölle is a PhD student in information systems at the University of Bamberg in Germany. His research interests center on privacy, ethics, and morality in the digital age. His work has been published in several conference proceedings, such as the *International Conference on Information Systems*, where his research was nominated for the Best Short Paper Award in 2024 and awarded 1st runner-up.

Marco Meier completed his PhD in information systems at the University of Bamberg. His research interests include the use of digital technologies in private (e.g., chatbots, video-on-demand services) and organizational contexts (e.g., telework, information security). His work has been published in *Information Systems Journal, Information & Management, Internet Research*, and *Communications of the Association for Information Systems.* His research was, among others, awarded the Magid Igbaria Outstanding Conference Paper of the Year Award at ACM SIGMIS CPR 2022 and nominated for the Claudio Ciborra Award at ECIS 2021 and the Best Short Paper Award at ICIS 2024. Off work, he likes traveling and skydiving.

Christian Maier is a professor at the University of Bamberg in Germany. His research interests include the IS use life cycle, especially the adoption, usage, and discontinuous usage of digital technologies in private and organizational use contexts. His research has been published, among others, in *MIS Quarterly* and *Information Systems Research*. He was awarded the Schmalenbach prize, the Early Career Awards by the AIS and the ACM SIGMIS, and the Heinz Maier-Leibnitz prize.