Computers in Human Behavior Reports 11 (2023) 100321

Contents lists available at ScienceDirect

Computers in Human Behavior Reports

journal homepage: www.sciencedirect.com/journal/computers-in-human-behavior-reports

We make a nice pair: Pairing the mID with a NeuroTechnology privacy enhancing technology improves mID download intentions

Dawn M. Lucier [a,*], Ryan T. Howell [a], Karynna Okabe-Miyamoto [b], Eric Durnell [b], Martin Zizi [b]

[a] Department of Psychology, San Francisco State University, United States
[b] Aerendir Mobile Inc, United States

ARTICLE INFO

Keywords:
Mobile identification
Technology acceptance
Privacy enhancing technology

ABSTRACT

Mobile identification (mID) allows users to prove identity across many situations like when traveling through an airport; however, the personally identifiable information in the mID, if mishandled, poses a great threat to privacy. One solution is NeuroTechnology privacy enhancing technologies (PETs), which can be paired with the mID to authenticate users using one's unique neuro-proprioceptive signals that are safer than traditional security methods like facial recognition. Across two studies, we explore how TAM constructs impact mID download intentions (DI) and how pairing the PET with the mID impacts DI. In Study 1 (N = 465), mID-specific privacy concerns, anxiety (mID-ANX), general privacy concerns, and perceived privacy risk (mID-PPR) were strong negative predictors of DI. In Study 2 (N = 420), pairing the NeuroTechnology PET with the mID led to decreased mID-PPR and mID-ANX, and increased DI. An experimental mediation model demonstrated that pairing the NeuroTechnology PET with the mID was linked to higher DI because of decreased mID-PPR and mID-ANX leading to greater mID positive attitudes. Because privacy concerns and anxiety are barriers to technology acceptance in the TAM literature, NeuroTechnology PETs provide a solution to reduce privacy concerns and anxiety, and improve technology adoption.

1. Introduction

Approximately a billion people in the world do not have proof of legal identity (World Bank Group &Global Partnership for Financial Inclusion, 2018). To address this, the United Nations and the World Bank started a global initiative called Identification for Development (ID4D), which aims to provide proof of identity globally by the year 2030 (Thales, 2022). Several countries are tackling the ID4D initiative by moving towards digital identification to provide easier access for citizens living in digitized public systems. In the U.S., there has been an increased push for digital identification, especially mobile identification (mID), with the Improving Digital Identity Act enacted in 2020, which established a task force to support states to create and implement frameworks to securely issue valid mIDs (Johnson, 2020). The transition to mIDs promises to provide a secure, touch-free way to prove identity, access services, and use various benefits with the added control to determine when and what types of information is shared based on the need of the situation.

1.1. Mobile identification (mID)

A significant benefit of the mID is the control that users have over the information that is shared when providing proof of identity, accessing services, or using various benefits. For example, if one uses a driver's license to verify one's age at a bar, there is no way to hide non-relevant information such as home address or license number; however, with a mID, one can show their date of birth but hide one's address when verifying one's age at a bar. This is type of feature provides privacy protection by allowing individuals to select what personally identifiable information is shown and is a type of privacy protection that cannot be achieved through physical identification documents (e.g., paper birth certificates, passports, and state-issued identifications). This type of privacy protection is extremely valuable because the personal information one's driver's license can be used to create fraudulent accounts or access existing accounts. The lack of privacy could also lead to threats to one's safety if one's personal address was used for a robbery or stalking.

* Corresponding author.
E-mail address: dlucier@sfsu.edu (D.M. Lucier).

https://doi.org/10.1016/j.chbr.2023.100321
Received 22 March 2023; Received in revised form 8 August 2023; Accepted 21 August 2023
Available online 22 August 2023

1.2. Privacy risks with the mID

As more states and countries transition to mIDs, concerns about the security and privacy of information may become a formidable obstacle to adoption. That is, because of the level of personally identifiable information that is housed in the mID, many may feel uncomfortable to use the mID, especially when physical forms of identification are standard. Recent research provides some insight into privacy trade-offs, revealing that users may accept the cost of the loss of privacy for the perceived benefits of the service or product (Distler, Lallemand, & Koenig, 2020; Vimalkumar, Sharma, Singh, & Dwivedi, 2021). As such, when exploring the barriers to adopting the mID, both the benefits and costs must be understood.

Although there are potential benefits to using the mID, these positives may be overshadowed by users' concerns with the new technology. Concerns with a new technology, also defined as technology anxiety, has been shown to negatively influence technology adoption (Oyman, Bal, & Ozer, 2022). Importantly, technology anxiety has been associated with privacy concerns (Osatuyi, 2015), both of which are negative predictors of the adoption of new technology. As such, another concern that can be an obstacle to mID adoption would be the perceived privacy risks that are inherent to the personal information housed within the mID, such as one's social security number, name, or date of birth.

Currently, mIDs rely on traditional security methods, such as passwords, thumbprint scanners, or facial recognition to protect users' privacy. However, although widely used, these traditional security measures are so inadequate in protecting, securing, and maintaining the privacy of one's personal information that they have resulted in more than 164 billion consumer records being exposed to identity theft and fraud in 2019 alone (House Oversight and Reform; Science, Space, and Technology; Ways and Means, 2022). Because of the high value nature of the personal information stored in mIDs, it is imperative to use improved methods of securing and protecting one's personal information.

1.3. Privacy enhancing technology (PET)

Privacy enhancing technologies (PETs) are technologies that are designed to protect an individual's personal data from unauthorized use and to protect their personally identifiable information (Fischer-Hbner & Berthold, 2017, p. 761). By using PETs in addition to traditional security methods used by the mID, such as a thumbprint scanner or facial identification, technologies can better protect personal data, secure personally identifiable information, and reduce perceived privacy risk.

Recent developments in PETs have offered reduction of risk by increasing user's privacy through neural tapping, which uses brain-linked signals to both recognize and shield an individual by using a physiologically generated bio-encryption. With this physiological identification method, the body becomes a million-character long password, also known as a NeuroTechnology or NeuroTech PET. NeuroTech PETs are used to identify and authenticate users using unique neuro-proprioceptive signals (Sodhro, Sennersten, & Ahmad, 2022) that can be read from the micro-vibrational patterns in one's hands. Physiological identification methods – not limited to neural tapping, but including heart rhythm and iris – are unique to the individual, which provides an extra layer of privacy protection that traditional biometric technologies cannot provide (Alsaadi, 2015). By using pairing NeuroTech PETs with the mID, the psychological factors of privacy concern and risk may be mitigated while the actual privacy of the mID can be strengthened by providing extra layers of physiologically-unique protection.

2. Theoretical framework

The Technology Acceptance Model (TAM) was introduced by Davis (1989) and has been described as a model that extends the Theory of Reasoned Action (TRA; Fishbein & Ajzen, 1977) and the Theory of Planned Behavior (TPB; Ajzen, 1991) to better understand the predictors of acceptance of new technologies (Park, Rhoads, Hou, & Lee, 2014), such as the mID. This model established specific internal and external constructs that examined technology acceptance and has since then been applied to other new technologies.

2.1. Internal TAM constructs

There are several internal TAM constructs that have been shown to be predictors of behavioral intention to use technology, however, in this current study, we focus on four specific constructs: Perceived usefulness, perceived ease of use, perceived ease of set-up, and positive attitude. Perceived usefulness (PU), or a user's subjective belief that a technology would be useful, along with perceived ease of use (PEOU) and perceived ease of set up (PEOSU), or a user's subjective expectation that the use of the technology or the set-up of the technology would be free of effort. Both PEOU and PEOSU have both been shown to be key predictors of behavioral intention of use (Davis, 1989). In fact, previous research has suggested that PU is one of the strongest predictors of behavioral intention to use mobile services and technologies (Haugstvedt & Krogstie, 2012; Oyman et al., 2022) and is positively associated with PEOU (Park et al., 2014). Additionally, positive attitudes towards a technology (PA) have also been shown to be a determinant of behavioral intention of use (Davis, 1989) and is defined as "positive affect that predicts behavioral intention to adopt technologies" (Davis, Bagozzi, & Warshaw, 1989). As such, we examine these four traditional TAM internal constructs.

2.2. External TAM constructs

Extensions to the TAM have included additional variables that might influence a user's perception and belief towards a technology. Because of the high risk for one's personally identifiable information to be compromised with the mID, we include external TAM constructs relating to privacy and technology anxiety to best understand intentions to use the mID.

One common way to measure privacy concerns is by examining general privacy concerns (GPC), which is defined as "general concerns for information privacy reflect their inherent needs and attitudes toward maintaining privacy, which are conceived to be more stable across domains or contexts" (Xu, Teo, Tan, & Agarwal, 2012). Current research suggests that general privacy concerns (GPC) do not influence individuals' intention to use or adopt technologies such as digital assistants (Vimalkumar et al., 2021) or apps (Fox, Clohessy, van der Werff, Rosati, & Lynn, 2021; Zhang, Luximon, & Li, 2022), however it is an important construct to measure as some individuals may be hesitant to use technology in general if they have high privacy concerns in general.

Importantly, it is especially vital to not only examine general privacy concerns, but also technology-specific privacy concerns. Context-specific privacy concerns or technology-specific privacy concerns (SPC) is an individual's concern with the loss of privacy as a result of engaging with a specific entity or technology (Xu et al., 2012). More specifically for our current study, mID-specific privacy concerns (mID-SPC), a cognitive phenomenon, focuses on individuals' beliefs and perceptions regarding the control, awareness, and confidence in the protective measures implemented by a specific vendor or service to safeguard personal information (Li, Sarathy, & Xu, 2011). Previous research has suggested that context-specific privacy concerns have a negative influence on behavioral intention to purchase technologies (Lin & Kim, 2016). As such, in addition to measuring general privacy concerns, we will also measure mID-specific privacy concerns.

Another facet of privacy concern is perceived privacy risk (PPR), which is defined as "the concern an individual would have regarding the potential compromise of their personal information" (Johnson, Kiser, Washington, & Torres, 2018, p. 115). PPR, another cognitive phenomenon, instead aims to capture individuals' perceptions of the potential

risks and negative consequences associated with disclosing personal information when using a specific technology (Li et al., 2011). Research has suggested that PPR with a specific technology is negatively associated with intentions to use technologies (Chang, Liu, & Shen, 2017; Sun, Wang, Shen, & Zhang, 2015). As such, we will measure privacy-specific risks associated with the mID.

A similar concept to PPR is technology anxiety (ANX), which is an individual's apprehension, or even fear, of using a technology (Demoulin & Djelassi, 2016, p. 5). PPR is an affective construct rather than a cognitive phenomenon like mID-specific privacy concerns and perceived privacy risk, which means that it focuses on the emotional outcomes of using a technology. Previous research has suggested that ANX has been negatively associated with intention to use and adoption of new technologies (Hsu, Wang, & Chiu, 2009; McFarland & Hamilton, 2006) and increases with concern for information privacy (Osatuyi, 2015). We will also measure mID technology anxiety to better understand psychological anxiety related to the mID.

Other external TAM constructs that may impact the adoption of the mID include social influence or having an innovative personality. Social influence (SI) is an individual's perception of usefulness from others and extensive research suggests SI has an influence on perceived usefulness (PU) or perceived each of use (PEOU) and behavioral intention to use (Akman & Mishra, 2015; Lu, Zhou, & Wang, 2009; Pan & Jordan-Marsh, 2010; Venkatesh, Morris, Davis, & Davis, 2003; Wu & Chen, 2017). Having an innovative personality (IP) is described as being curious about new technology and perceiving technology as being easy to use and useful, which has positive influence on user's PU and PEOU (Sun & Chi, 2019; Yuan, Lin, & Zhuo, 2016).

3. Conceptual model and hypotheses

To overcome the vulnerabilities inherent with the traditional security methods used by the mID (e.g., facial recognition), pairing these traditional authentication methods with a NeuroTech PET, may not only make using the mID safer, but it also may reduce the psychological concerns of privacy risk and technology anxiety of users. This in turn may aid in the adoption of the mID and thus, can be used to build a framework of adoption for any new technology along with the traditional TAM constructs. As such, the present research aims to address the gaps in the literature on technology acceptance through the lens of the three dimensions of privacy (i.e., general privacy concerns, technology specific privacy concerns, and perceived privacy risk) and the psychological characteristics of privacy risk (cognitive) and technology anxiety (affective). Our unique contribution to this area of research includes testing a solution to technology acceptance by pairing a new technology (mID) with a NeuroTech PET to mitigate the negative effects of perceived privacy risks (PPR) and technology anxiety (ANX) on download intention (DI).

In the present research, we extend the traditional internal TAM constructs by including privacy concern, technology anxiety, and personality-focused external TAM constructs to better understand the cognitive and affective factors that affect the adoption of the mID, a new technology that has not been explored using the TAM. Additionally, our study aligns with the existing literature that employs hypothetical scenarios or descriptions to assess participants' intention to use a specific technology. Several studies have utilized similar research methodologies, emphasizing the importance of understanding individuals' intentions to use a technology based on hypothetical scenarios or descriptions. For example, James, Pirim, Boswell, Reithel, and Barkhi (2008) extended the TAM to measure the intention to use biometric devices by having participants read vignettes (e.g., Jimmy utilizes a biometric hand geometry scanner as a means of access control to his home). The researchers demonstrated two important, positive relationships between the perceived usefulness of the security technology and perceived ease of use of the security technology on intention to use the security technology. Guinea, Stang, Nitsche, and Sax (2021) revealed a significant difference in user acceptance between two groups: participants who read the vignette about highly automated comfort functions reported significantly higher user acceptance when compared to the group of participants who read the vignette about fully automated comfort functions. Taking inspiration from these studies that use hypothetical scenarios, our current research will also use hypothetical scenarios aided with visual images to ensure participants are able to fully understand mIDs and biotech PETs.

To better understand the basic download intentions of the mID, we recruited a sample of adults to respond to a survey describing the mID and to answer questions regarding our internal and external TAM constructs (Study 1). Specifically, the goal of Study 1 was to use a correlational design to determine the impact of our external TAM constructs such as mID-SPC, GPC, mID-ANX, and mID-PPR in predicting mID download intentions. Because of the barrier to use or engage with a technology that is connected with having privacy concerns (Lin & Kim, 2016), in Study 2 we conducted an experiment and a 2 $\times$ 2 factorial design to determine whether providing warnings about privacy (or not) and whether pairing the mID with a Privacy Enhancing Technology (PET; or not) impacted download intentions for the mID. As such, the goals of Study 2 were to determine if pairing a PET with the mID would impact our external TAM constructs such as mID-SPC, mID-PPR, and mID-ANX, as well as determine if pairing a PET with the mID would impact the internal TAM constructs. Importantly, we aimed to test if these decreases in mID-SPC, mID-PPR, and mID-ANX mediate the increases in the TAM constructs when paired with a PET. Please refer to the Methods section and Appendix B for a detailed description of the specific measures and vignettes used in each study.

To explore whether our external TAM constructs (e.g., mID-SPC, GPC) impact download intention and whether pairing a Privacy Enhancing Technology may improve download intentions by alleviating our external TAM constructs, we have created multiple hypotheses that are supported by previous research.

H1. Perceived Ease of Set-Up (PEOSU), Perceived Ease of Use (PEOU), Perceived Usefulness (PU), and Positive Affect (PA) will all be positively associated with Download Intentions (DI)

H2. General Privacy Concerns (GPC), mID-Specific Privacy Concerns (mID-SPC), mID-Specific Privacy Risk (mID-PPR), and mID-Specific Anxiety (mID-ANX) will be negatively associated with Download Intentions (DI)

H3. Innovative Personality (IP) and Social Influence (SI) will be positively associated with Download Intentions (DI)

Previous research has demonstrated that perceived ease of set-up (PEOSU), perceived ease of use (PEOU), perceived usefulness (PU), and positive affect (PA) are all strong predictors of behavioral intention to use (Davis, 1989; Davis et al., 1989; Haugstvedt & Krogstie, 2012; Lin & Kim, 2016; Oyman et al., 2022; Park et al., 2014; Park, Lee, & Cheong, 2007). In our study, we refer to PEOSU, PEOU, PU, and PA as our internal TAM constructs. Research has also found that general privacy concerns (GPC), technology-specific privacy concerns, perceived privacy risk (PPR), and technology anxiety all impact behavioral intention to use, or in our study, download intentions (DI; Demoulin & Djelassi, 2016; Gu, Xu, Xu, Zhang, & Ling, 2017; Johnson et al., 2018; Xuet al., Agarwal & Prasad, 1999). Furthermore, innovative personality (IP) and social influence (SI) also positive influence download intentions (DI; Sun & Chi, 2019).

H4. Download Intentions (DI) will increase when the mID is paired with the Privacy Enhancing Technology (PET)

H5. The internal constructs of PEOSU, PEOU, PU, and PA will increase when the mID is paired with the Privacy Enhancing Technology (PET)

H6. The external constructs of General Privacy Concerns (GPC), mID-Specific Privacy Concerns (mID-SPC), mID-Specific Privacy Risk (mID-

PPR), and mID-Specific Anxiety will decrease when the mID is paired with the Privacy Enhancing Technology (PET)

Research has shown that privacy concerns and technology anxiety interfere with the adoption and use of new technologies (Johnson et al., 2018; Lin & Kim, 2016; Liu & Tao, 2022; Zhang, Luximon, & Li, 2022; McFarland & Hamilton, 2006; Park et al., 2014). Because privacy concerns and anxiety about new technologies are barriers to adoption, we hypothesize that pairing the mID with a PET may mitigate anxiety and privacy concerns, which will in turn improve mID download intentions.

4. Study 1

4.1. Participants

We aimed to recruit 100 participants per condition based on sample sizes in previous literature using similar vignettes and experimental designs (target N = 400; Gu et al., 2017; Horne & Przepiorka, 2021; Liao, Lin, & Chen, 2023; Fraley & Vazire, 2014). A total of 465 participants were recruited from Amazon Mechanical Turk via Turkprime and received $0.70 for their participation. A total of 12 participants were dropped from all analyses – 11 for not passing our three attention checks and one for being outside of the United States. Thus, the final sample size was $N = 453$. In addition to completing the full survey (see description of measures below), participants reported their age ($M_{age} = 41.62$; $SD_{age} = 13.39$), gender (49% female; 49% male), ethnicity (72% Caucasian/White), household income (47% had HHI greater than $60,000), and education (58% with a college degree or higher). They also reported if they currently use a mobile wallet (an app similar to the mID) on their smartphone, with 48% of the sample reporting they did.

4.2. Procedures

In Study 1, a convenience sample was recruited from Amazon Mechanical Turk via Turkprime. Participants were provided with information about the Mobile ID (mID) app, which "serves as an electronic identifier for proving identity, age, and driving status." Following this, participants rated their agreement on a 5-point Likert scale (1 = strongly disagree; 5 = strongly agree) with the four internal constructs of perceived ease of set-up, ease of use, perceived usability, positive attitudes, and download intentions. Additionally, participants provided ratings on six external variables: general privacy concern, mID-specific privacy concerns, mID-specific risk assessment, mID-specific anxiety, innovative personality, and social influence.

Participants first consented to the study. Next, they were asked about their familiarity with various cyberpsychology terms. Specifically, we asked if they knew the meaning of data encryption, biometric authentication, mobile device authentication, and user authentication. For any term the participant answered as "maybe" or "no," we provided a definition for each (see Appendix A). Then, participants read about a "new Mobile ID app" by viewing four graphics that included both verbal and graphical narratives (see Appendix B, slides 1–4).

After viewing the mID graphics, participants were told "in the next section, you will answer questions only about this Mobile ID app." In this section, we had participants rate their level of agreement with five internal TAM constructs as well as six external variables. First, participants rated their level of agreement with items which assessed the five internal TAM constructs: Perceived ease of set-up (PEOSU), perceived ease of use (PEOU), perceived usefulness (PU), positive attitudes (PA), and download intentions (DI). Second, participants rated their level of agreement with items which assessed the six external variables: general privacy concern (GPC), mID-specific privacy concerns (mID-SPC), mID-specific perceived privacy risk (mID-PPR), mID-specific anxiety (miD-ANX), innovative personality (IP), and social influence (SI; see construct description below). When evaluating reliability coefficients, the following values were interpreted as: (1) less than 0.70 as below traditional thresholds for adequate reliability, (2) between 0.70 and 0.79 as "adequate" reliability, (3) 0.80 - 0.89 as "good" reliability, and (4) greater than or equal to 0.90 as "excellent" reliability.

4.3. The four internal TAM constructs

In line with previous research, we are examining the following four internal TAM constructs.

4.3.1. Perceived ease of set-up (PEOSU)

For our TAM model we measured participants' PEOSU for the mID (i.e., before the participant would use the mobile ID in their day-to-day life). In order to measure PEOSU, we asked participants to rate five items (1 = *strongly disagree*; 5 = *strongly agree*). First, they rated two items with the sentence stem "*It would be easy for me to*" (1) scan a government-approved ID document into this Mobile ID app ($M = 4.07$, $SD = 0.81$) and (2) upload a photo from my photo library or add a selfie into this Mobile ID app ($M = 4.13$, $SD = 0.82$). We also asked participants to rate three items with the sentence stem "*I am confident that I could add*" (3) an electronic signature to this Mobile ID app ($M = 4.05$, $SD = 0.81$), (4) my physical ID to my phone using this Mobile ID ($M = 4.17$, $SD = 0.77$), and (5) personal medical records to this Mobile ID app ($M = 3.83$, $SD = 0.96$). Overall, participants rated the mID as easy to set up. For example, 84% of participants reported scanning a government-approved ID document into my mID app would be easy. To score PEOSU we calculated the average of the five items. Overall, the scale demonstrated adequate reliability ($M = 4.05$, $SD = 0.77$; $\alpha = 0.85$).

4.3.2. Perceived ease of use (PEOU)

We also measured the more traditional PEOU of the mID. In order to measure PEOU, we asked participants to rate six items (1 = *strongly disagree*; 5 = *strongly agree*). First, they rated three items with the sentence stem "*It would be easy for me to*" (1) authenticate my identity securely when using an online service using this Mobile ID app ($M = 4.11$, $SD = 0.78$), (2) add this Mobile ID app to my phone ($M = 4.32$, $SD = 0.70$), and (3) complete a real-time online ID check on my Mobile ID app with banks, businesses, and governments ($M = 4.10$, $SD = 0.76$). We also asked participants to rate three items with the sentence stem "*I am confident that I could*" (4) digitally sign documents with my mID app ($M = 4.02$, $SD = 0.81$), (5) buy age-restricted items by confirming my legal age without sharing this address with this Mobile ID app, ($M = 4.09$, $SD = 0.86$), and (6) use this Mobile ID instead of a physical ID. Overall, participants rated the mID as easy to use ($M = 4.14$, $SD = 0.87$). For example, 79% of participants reported they are confident they could digitally sign documents with the mID app. Also, 82% reported they are confident they could buy age-restricted items by confirming my legal age without sharing my address with my mID app. To score PEOU we calculated the average of the six items. Overall, the scale demonstrated good reliability ($M = 4.13$, $SD = 0.64$; $\alpha = 0.89$).

4.3.3. Perceived usefulness (PU)

In order to measure PU we asked participants to rate four items (1 = *strongly disagree*; 5 = *strongly agree*) which all began with the sentence stem "*Overall, I find the mobile ID useful*" (1) verify identity when picking up prescriptions and buying over-the-counter medications that require proof of age ($M = 4.07$, $SD = 0.89$), (2) access bank services (opening accounts, deposits, transfers; $M = 3.90$, $SD = 1.00$), (3) store and share important credentials (work IDs, vehicle registration, auto insurance, education certificates; $M = 4.06$, $SD = 0.92$), (4) to make purchases without signatures or PINs (restaurant to-go orders, grocery stores; $M = 3.90$, $SD = 1.00$). Overall, participants rated the mID as useful. For example, 82% of participants reported they find the mID useful to store and share important credentials (work IDs, vehicle registration, auto insurance, education certificates). To score PU we calculated the average of the four items. Overall, the scale demonstrated good reliability ($M = 3.98$, $SD = 0.83$; $\alpha = 0.90$).

4.3.4. Positive attitudes (PA)

In order to measure PA, we asked participants to provide their ratings to two questions which were identical except the response options, "Overall, how would you rate your overall attitude towards using a Mobile ID?" with two sets of response options: (a) 1 = *unattractive* to 5 = *attractive* ($M = 3.75$, $SD = 1.15$) and (b) 1 = *unfavorable* to 5 = *favorable* ($M = 3.76$, $SD = 1.19$). Also, participants rated their level of agreement (1 = *strongly disagree*; 5 = *strongly agree*) with two other items: (3) It seems that a mID would be relevant to me ($M = 3.78$, $SD = 1.11$) and (4) it seems that a mID would be meaningful ($M = 3.66$, $SD = 1.08$). Interestingly, when compared to the high PESU, PEOU, and PU ratings, participants were less likely to report PA towards the mID. For example, only 69% of participants reported they found the mID attractive. To score PA we calculated the average of the four items. Overall, the scale demonstrated excellent reliability ($M = 3.74$, $SD = 1.05$; $\alpha = 0.95$).

4.4. The six external TAM constructs

Because of the privacy risks associated with the mID, most of our external TAM constructs center around perceptions of privacy and anxiety. These external TAM constructs are central to the goal of study as previous research has demonstrated the important distinction between general and technology-specific privacy concerns on intentions to use (Lin & Kim, 2016). As such, we are measuring the following constructs.

4.4.1. General privacy concern (GPC)

In order to measure GPC, we asked participants to rate three items (1 = *strongly disagree*; 5 = *strongly agree*): (1) I am sensitive to privacy-related issues ($M = 4.05$, $SD = 0.84$), (2) to me, it is important to protect privacy ($M = 4.40$, $SD = 0.65$), and (3) I am generally concerned about potential privacy threats ($M = 4.20$, $SD = 0.76$). Overall, participants reported high levels of GPC. For example, 94% of participants agreed that it is important to protect privacy. To score GPC we calculated the average of the three items. Overall, the scale demonstrated excellent reliability ($M = 4.22$, $SD = 0.66$; $\alpha = 0.86$).

4.4.2. mID-specific privacy concerns (mID-SPC)

In order to measure mID-SPC, we asked participants to rate four items (1 = *strongly disagree*; 5 = *strongly agree*): (1) I worry that this Mobile ID app will leak my personal information to irrelevant third-parties ($M = 3.45$, $SD = 1.22$), (2) if I were to download and use this app, I would be concerned that the Mobile ID app would violate my privacy ($M = 3.42$, $SD = 1.24$), (3) if I were to download and use this app, I would be concerned that the Mobile ID app would misuse my personal information ($M = 3.36$, $SD = 1.25$), and (4) I think this Mobile ID app will over-collect my personal information ($M = 3.34$, $SD = 1.26$). Although participants reported high levels of GPC, participants reported lower mID-SPC. For example, only 57% of participants agreed that they worried "that this Mobile ID app will leak my personal information to irrelevant third-parties." To score mID-SPC we calculated the average of the four items. Overall, the scale demonstrated excellent reliability ($M = 3.39$, $SD = 1.18$; $\alpha = 0.96$).

4.4.3. mID-specific perceived privacy risk (mID-PPR)

In order to measure mID-PPR, we asked participants to rate three items (1 = *strongly disagree*; 5 = *strongly agree*): (1) Others may know information about my online transactions if I use this Mobile ID app ($M = 3.28$, $SD = 1.12$), (2) there is a significant risk when making my queries and/or my banking transactions through this Mobile ID app ($M = 3.27$, $SD = 1.15$), and (3) I believe that making queries and/or banking transactions with this Mobile ID app is a risky choice ($M = 3.29$, $SD = 1.16$). Similar to the lower levels of mID-SPC, participants reported relatively lower levels of mID-PPR. For example, only 49% of participants agreed "others may know information about my online transactions if I use this Mobile ID app" and 47% agreed that "making queries and/or banking transactions with this Mobile ID app is a risky choice." To score mID-PPR we calculated the average of the three items. Overall, the scale demonstrated excellent reliability ($M = 3.28$, $SD = 1.06$; $\alpha = 0.92$).

4.4.4. mID-specific anxiety (mID-ANX)

In order to measure mID-ANX, we asked participants to rate four items (1 = *strongly disagree*; 5 = *strongly agree*): (1) The information I provide when I use this Mobile ID app to pay for purchases may not be confidential ($M = 3.36$, $SD = 1.10$), (2) there is a great risk of breach of privacy with payments using this Mobile ID app ($M = 3.36$, $SD = 1.19$), (3) I have concerns about the security of paying for purchases using this Mobile ID app ($M = 3.42$, $SD = 1.17$), and (4) I may lose control of my personal information if I pay for purchases with this Mobile ID app ($M = 3.33$, $SD = 1.14$). In line with the lower ratings of mID-SPC and mID-PPR, participants reported relatively lower levels of mID-ANX. For example, 50% of participants agreed that "making queries and/or banking transactions with this Mobile ID app is a risky choice." To score mID-ANX we calculated the average of the four items. Overall, the scale demonstrated excellent reliability ($M = 3.37$, $SD = 1.07$; $\alpha = 0.94$).

4.4.5. Innovative personality (IP)

In order to measure IP, we asked participants to rate three items (1 = *strongly disagree*; 5 = *strongly agree*): (1) I like to experiment with new ways of doing things ($M = 3.69$, $SD = 0.93$), (2) I like to take a chance ($M = 3.17$, $SD = 1.10$), and (3) I like to be around unconventional people who dare to try new things ($M = 3.25$, $SD = 1.04$). To score IP we calculated the average of the three items. Overall, the scale demonstrated excellent reliability ($M = 3.37$, $SD = 0.90$; $\alpha = 0.85$).

4.4.6. Social influence (SI)

In order to measure SI, we asked participants to rate three items (1 = *strongly disagree*; 5 = *strongly agree*): (1) I find mobile apps useful in my daily life ($M = 4.17$, $SD = 0.87$), (2) using mobile apps helps me accomplish things more quickly ($M = 4.12$, $SD = 0.89$), (3) using mobile apps enhances my effectiveness on the job ($M = 3.80$, $SD = 1.07$). To score SI we calculated the average of the three items. Overall, the scale demonstrated excellent reliability ($M = 4.03$, $SD = 0.87$; $\alpha = 0.90$).

4.5. Outcome variable

4.5.1. Download intentions (DI)

In order to measure DI, we asked participants to rate three items (1 = *strongly disagree*; 5 = *strongly agree*): (1) I am willing to download the mID app ($M = 3.55$, $SD = 1.19$), (2) after reading the related information of the mID app, I am willing to try the mID app ($M = 3.60$, $SD = 1.22$), (3) after reading the related information of the mID app, I am willing to consider the mID app as a preferred app to download in the personal identification app category ($M = 3.57$, $SD = 1.21$). In line with the lower PA, participants were less likely to report download intentions for the mID when compared with the PESU, PEOU, and PU ratings. For example, only 63% of participants reported they were willing to try mID app after reading about it. To score DI we calculated the average of the three items. Overall, the scale demonstrated excellent reliability ($M = 3.57$, $SD = 1.17$; $\alpha = 0.97$).

5. Results

5.1. Correlations among internal TAM constructs, external TAM constructs, and DI

To test H1, H2, and H3, we examined the intercorrelations within the internal TAM constructs, the external TAM constructs, and DI. All internal constructs were significantly correlated with every other internal construct (i.e., PEOSU and PEOU $r = .79$; PEOU and PU $r = .75$; PU and PA $r = .65$; PEOSU and PU $r = .64$) though some of the constructs were more moderately correlated (i.e., PEOSU and PA $r = .48$; PEOU and PA r

= .51). Importantly, in line with H1, PEOSU ($r = 0.44$), PEOU ($r = 0.48$), PU ($r = 0.57$), and PA ($r = 0.86$) were all positively associated with DI.

Next, the three mID-specific variables, mID-SPC, mID- PPR, and mID-ANX were all highly correlated (r's ranging from 0.79 to 0.85), indicating very similar ratings for each. Supporting H2, DI was significantly negatively associated with GPC ($r = -0.16$), mID-SPC ($r = -0.58$), mID-PPR ($r = -0.53$), and mID-ANX ($r = -0.56$). These correlations are notable, as the association between GPC and DI, while significant, was much weaker than the correlation between mID-SPC and DI. This highlights the important role that mID-SPC plays in DI and supports previous research (Lin & Kim, 2016). As a matter of fact, when DI were regressed onto both GPC and mID-SPC, there was no effect of GPC. Though, interestingly, GPC did act as a moderator of the association between mID-SPC and DI being strongest for those with the greatest GPCs.

Additionally, the two individual difference variables, IP and SI was moderately correlated ($r = 0.39$). To test H3, we examined the correlations between the two individual difference variables and DI. Both correlations were positive and statistically significant. Specifically, DI was positively associated with IP ($r = 0.41$) and SI ($r = 53$).

5.2. Predicting DI From the external TAM constructs

Given the strong associations among mID-specific privacy concerns (mID-SPC), mID-specific perceived privacy risk (mID-PPR), and mID anxiety (mID-ANX), we examined the individual effects of mID-SPC, mID-PPR, and mID-ANX in predicting download intentions (DI) after controlling for general privacy concerns (GPC), innovative personality (IP), and social influence (SI; collectively). That is, we regressed DI onto GPC, IP, and SI as well as mID-SPC (model 1), mID-PPR (model 2), and mID-ANX (model 3). First, as expected by the low intercorrelations among GPC, IP, and SI, all three predictors were significant predictors of DI ($b = -.16$, $b = 0.23$, and $b = 0.45$, respectively with $p < .001$ for all three predictors) before entering mID-SPC, mID-PPR, and mID-ANX into the regression models. Second, even when controlling for GPC, IP, and SI, all three mID-specific variables predicted significant decreases in DI: $b = -.42$, $p < .001$ for mID-SPC (model 1), $b = -0.39$ $p < .001$ for mID-PPR (model 2), and $b = -0.40$, $p < .001$ for mID-ANX (model 3) (see Fig. 1).

Third, while GPC was not a significant predictor of DI in model 1, model 2, or model 3 (after adding mID-SPC, mID-PPR, or mID-ANX as predictors) we did determine that GPC was a significant and consistent moderator of the strong negative relationship among mID-SPC, mID-PPR, and mID-ANX with DI. Specifically, in each model, those with the highest GPC, compared to those with the lowest GPC, had the strongest negative associations among mID-SPC, mID-PPR, and mID-ANX with DI. For example, see Fig. 4 where we displace how the relations between mID-PPR and DI is strongest for those with the highest GPC (Mean + 1SD $b = -0.51$; $SE = 0.05$; $p < .001$) whereas the relations is weaker for those with the lowest GPC (Mean-1SD $b = -0.30$; $SE = 0.06$; $p < .001$). As such, we found further support for H2, with particular support for the importance that mID-SPC playing the strongest role on DI, especially among those with the highest GPC (see Fig. 2).

6. Brief discussion

The main goal of Study 1 was to examine how the external TAM factors impacted mID download intention (DI). Interestingly, the associations between general privacy concern (GPC) and the five internal TAM constructs were weak, and not significantly related to DI when controlling for any of the mID-specific variables (i.e., mID-SPC, mID-PPR, and mID-ANX). Importantly, it appears that mID-specific privacy concerns (mID-SPC) play a large role on DI, which provides guidance on how to improve DI for the mID. Given the weak associations between the TAM constructs and GPC, the focus for future TAM studies should assess how to reduce technology-specific privacy concerns and anxiety. Therefore, in Study 2, we provide a solution to reduce the concern with privacy and anxiety through the pairing of a privacy enhancing technology (PET) with the mID.

7. Study 2

To build off of Study 1, the goal of the first study was to determine if pairing a PET with the mID would decrease mID-specific privacy concerns (mID-SPC), mID-specific perceived privacy risk (mID-PPR), and mID-specific anxiety (mID-ANX) as well as would increase the internal TAM constructs, and test if these decreases in mID-SPC, mID-PPR, and mID-ANX mediate the increases in the TAM constructs when paired with a PET.

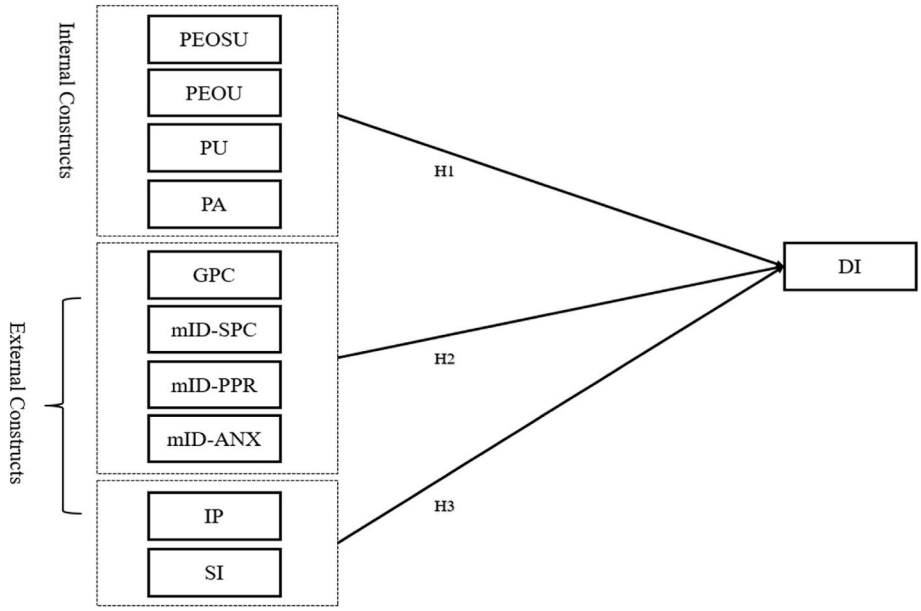


Fig. 1. Research model (H1 – H3).

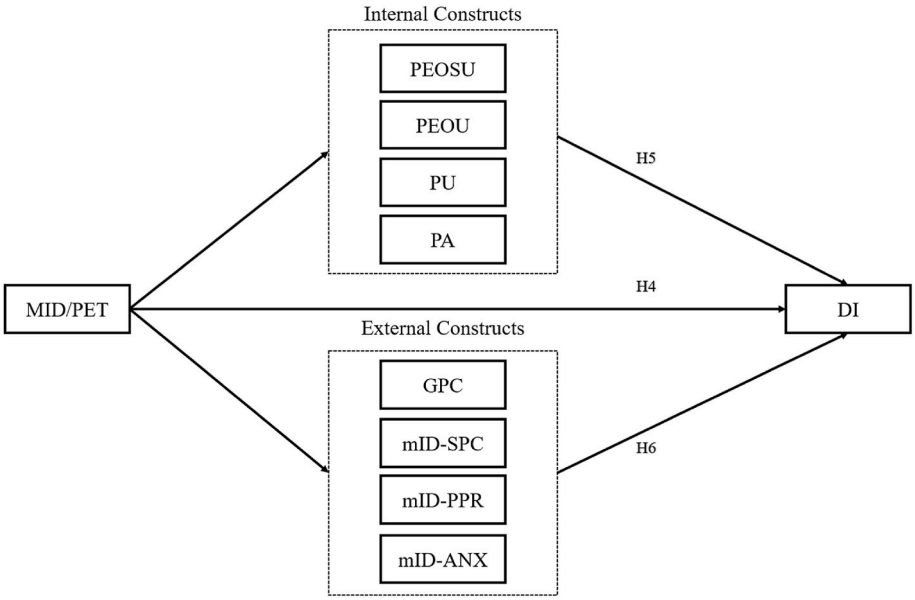


Fig. 2. Research model 2 (H4 – H6).

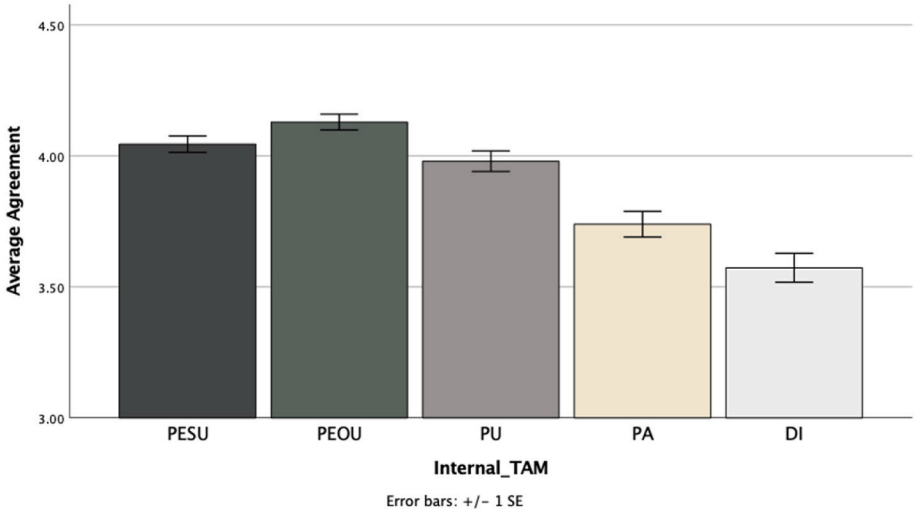


Fig. 3. Average agreement for internal TAM constructs. *Note.* For the internal TAM constructs PEOSU = Perceived Ease of Set-Up. PEOU = Perceived Ease of Use. PU = Perceived Usefulness. PA = Positive Attitudes Toward mID. DI = mID Download Intentions. In Fig. 3 we report the average level of agreement with each internal TAM construct. We examined the differences in the pattern of means with a one-way within-subjects ANOVA, which was statistically signification (F [4, 1804] = 71.07, p < .001]. Post-hoc mean comparison with Bonferroni corrected p-values, demonstrated, all pairwise comparisons were statistically significant with a lone exception: the average agreement with PESU and PU was not statistically different (p = .358).

7.1. Participants

Participants from Study 2 (N = 420) were recruited from Amazon Mechanical Turk via Turkprime and received $0.70 for their participation. Participants reported their age (M_{age} = 40.88; SD_{age} = 12.33), gender (42% female; 56% male), ethnicity (76% Caucasian/White), household income (45% had HHI greater than $60,000), and education (53% with a college degree or higher). They also reported if they currently use a mobile wallet on their smartphone, with 48% of the sample reporting they did.

7.2. Procedures

For Study 2, an independent convenience sample was recruited from Amazon Mechanical Turk via Turkprime. The study employed an online vignette experiment, using a 2 × 2 between-subject factorial design. Participants were randomly assigned to one of four conditions resulting from the combination of two factors. Factor 1 involved the presence or absence of a security warning (warning condition vs. no warning condition), while Factor 2 involved the presence or absence of a privacy-enhancing technology (PET condition vs. no PET condition). Participants assigned to the warning condition received a warning statement highlighting the vulnerabilities of current physical biometric technology, whereas participants assigned to the PET condition were informed that the mID was paired with a privacy-enhancing technology referred to as "BioTech" or "NeuroTech," providing enhanced security measures. The sample size for Study 2 included approximately 100 participants per condition, resulting in a total sample size of N = 420 participants.

The same cyberpsychology terms as in Study 1 were defined for the participants, they read "*in the next section, we will discuss a new technology called Mobile Identification by showing you 4 slides that describe this technology. Later we will have you rate your understanding and attitudes toward this technology*." Participants all read about the mID by viewing four slides that included both verbal and graphical narratives (see Appendix B, slides 1–4). Next, participants were randomly assigned to be primed about mID privacy concerns or not primed. For example, those primed to be concerned about the privacy risk when using the mID read "the current ***physical biometric technology*** on smartphones can be ***hacked, recorded, or stolen***. This lack of security leaves you ***vulnerable to identity fraud*** including financial, medical, or identity theft" (Appendix

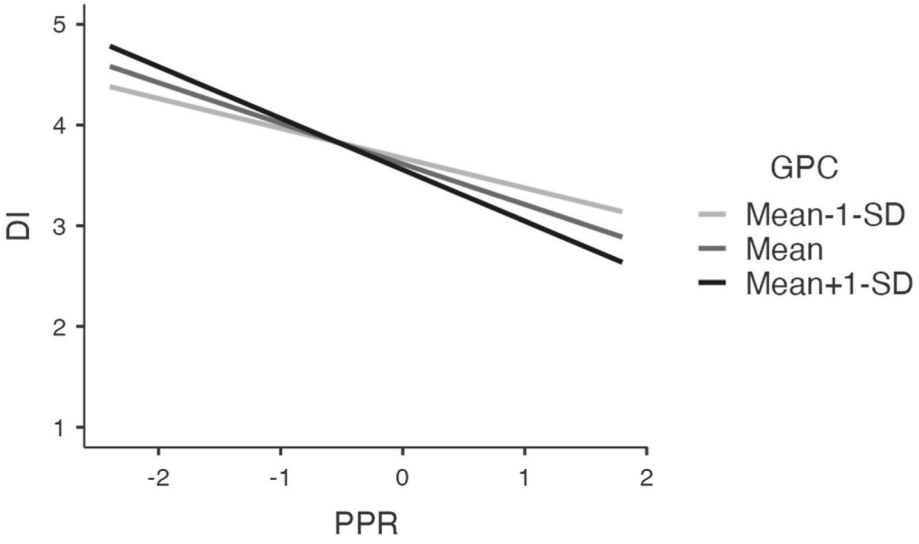


Fig. 4. Relations between perceived privacy risk and general privacy concerns. *Note*. For the internal TAM constructs DI = Download Intentions. For the external TAM constructs: General Privacy Concern = GPC; mID-Specific Perceived Privacy risk = mID-PPR. In Fig. 4 we displace how the relations between mID-PPR and DI is strongest for those with the highest GPC (Mean + 1SD $b = -0.51$; SE = 0.05; $p < .001$) whereas the relations is weaker for those with the lowest GPC (Mean-1SD $b = -0.30$; SE = 0.06; $p < .001$).

B, slide 7). The participants not assigned to be primed about mID privacy concerns did not read this warning nor see the graphical narrative on the slides. Finally, participants were randomly assigned to read a vignette about the mID alone or a vignette pairing the mID with the NeuroTech PET. For example, those who were randomly assigned to the vignette pairing of the mID with the NeuroTech PET, read that the mID had been paired, at no cost, with a privacy enhancing technology (e.g., a PET which we called "NeuroTech"): "by pairing the ***Mobile ID app*** with ***BioTech***, your private information and data are better protected compared to other biometric technologies because ***your unique brain cortex signals are not possible to hack***" (Appendix B, slides 8–10). Thus, participants were randomly assigned to read about a new mID technology with (1) a warning about privacy theft (i.e., the "warning condition"): or not (i.e., the "no warning condition") and (2) being paired with a PET called NeuroTech (i.e., the "PET condition") or not (i.e, the "no PET condition"). Participants then rated their level of agreement with five internal TAM constructs as well as six external TAM constructs.

After viewing the mID slides based on their assigned conditions, participants were told "*in the next section, you will answer questions only about this Mobile ID app.*" First, participants rated their level of agreement with items which assessed the same five internal TAM constructs from Study 1: Perceived ease of set-up (PEOSU), perceived ease of use (PEOU), perceived usefulness (PU), positive attitudes (PA), and download intentions (DI). Second, participants rated their level of agreement with items which assessed the six external TAM constructs: General privacy concerns (GPC), mID-specific privacy concerns (mID-SPC), mID-specific perceived privacy risk (mID-PPR), mID-specific anxiety (mID-ANX), innovative personality (IP), and social influence (SI). As was true when evaluating reliability coefficients from Study 1, the following values were used for interpretations of reliability: (1) less than 0.70 as below traditional thresholds for adequate reliability, (2) between 0.70 and 0.79 as "adequate" reliability, (3) 0.80 - 0.89 as "good" reliability, and (4) greater than or equal to 0.90 as "excellent" reliability. Because the same items and response options were used for the all the TAM constructs, in the section below we only report the descriptive statistics for each construct.

7.3. The four internal TAM constructs: PEOSU, PEOU, PU, and PA

Participants rated their agreement (1 = *strongly disagree*; 5 = *strongly agree*) with the items in order to measure four different internal TAM constructs. Specifically, participants rated their level of agreement with items adapted to assess PEOSU (e.g., "*I am confident that I could add my physical ID to my phone using this Mobile ID*"; $M = 4.09$, $SD = 0.66$, $\alpha = 0.85$), PEOU (e.g., "*I am confident I could use this Mobile ID instead of a physical ID*"; $M = 4.13$, $SD = 0.68$, $\alpha = 0.89$), PU (e.g., "*Overall, I find this mobile ID useful to access bank services*"; $M = 4.03$, $SD = 0.82$, $\alpha = 0.90$), and PA (e.g., "*It seems that this Mobile ID would be relevant to me*"; $M = 3.65$, $SD = 1.05$, $\alpha = 0.95$). Overall, the five internal TAM constructs demonstrated good to excellent reliability. The inter-correlational patter of the four internal constructs was similar to Study 1. For example, all constructs were significantly correlated with every other construct (i.e., PEOSU and PEOU $r = .78$; PEOU and PU $r = .63$; PU and PA $r = .62$; PEOSU and PU $r = .60$) though some of the constructs were more moderately correlated (i.e., PEOSU and PA r = .44; PEOU and PA $r = .47$).

7.4. The six external TAM constructs: GPC, mID-SPC, mID-PPR, mID-ANX, IP, and SI

Participants rated their level of agreement with items adapted to assess GPC (e.g., "*To me, it is important to protect privacy.*" $M = 5.22$, $SD = 0.71$, $\alpha = 0.87$), mID-SPC (e.g., "*If I were to download and use this app, I will be concerned that Mobile ID app would violate my privacy.*" $M = 3.45$, $SD = 1.16$, $\alpha = 0.95$), mID-PPR (e.g., "*I believe that making queries and/or banking transactions with this Mobile ID app is a risky choice.*" $M = 3.29$, $SD = 1.07$, $\alpha = 0.92$), mID-ANX (e.g., "*I may lose control of my personal information if I pay for purchases with a Mobile ID app*" $M = 3.33$, $SD = 1.06$, $\alpha = 0.93$), IP (e.g., "*I like to be around unconventional people who dare to try new things.*" $M = 3.36$, $SD = 0.90$; $\alpha = 0.82$), and SI (e.g., "*Using mobile apps helps me accomplish things more quickly.*" $M = 3.99$, $SD = 0.91$; $\alpha = 0.89$). Overall, the six external TAM constructs demonstrated good to excellent reliability. The inter-correlational patter of the five internal constructs was similar to Study 1. For example, the three mID-specific variables (i.e., mID-SPC, mID-PPR, and mID-ANX) were all highly correlated (r's ranging from 0.78 to 0.83). Also, the general external constructs (i.e., GPC, IP, and SI) were all significantly, but modestly, correlated with the three mID-specific constructs (r's ranging from −.13 to .39). Finally, a general privacy concern was not correlated with an IP ($r = -0.08$, $p = .093$) nor SI ($r = 0.04$, $p = .420$).

7.5. Outcome variable: DI

Like Study 1, participants in Study 2 also rated their agreement (1 = *strongly disagree*; 5 = *strongly agree*) with the mID DI measure (e.g., "*I am willing to download this Mobile ID app*"; $M = 3.48$, $SD = 1.18$, $\alpha = 0.97$).

8. Results

8.1. The association between external and internal TAM constructs and DI

We first wanted to examine the regression coefficients with the external TAM constructs predicting the internal TAM constructs. Because all these TAM constructs were measured after being randomly assigned to either the: (1) NeuroTech PET or No NeuroTech PET as well as the (2) Warning or No warning conditions, we examined these associations with five regression models for each external privacy constructs. In each regression model we predicted the internal TAM constructs and DI from (a) the external TAM construct, (b) the two experimental conditions, and (c) the interactions between the external TAM construct and the two experimental conditions. For example, we first predicted PEOSU from: (a) GPC, (b) the effects of the two experimental conditions, and (c) the interactions between GPC X NeuroTech PET as well as GPC X Warning. In this model, there as one significant predictor: GPC was a significant predictor of increased PEOSU ($b = 0.15$, $p = .006$). That is, those who had GPC reported the mID would be easier to set up. Importantly, this positive association was not moderated by the two experimental conditions.

Overall, GPC did have a consistent, albeit small, association with the internal TAM constructs. For example, GPC was a significant predictor of increased PEOU ($b = 0.12$, $p = .029$) and decreased PA ($b = -0.16$, $p = .002$). GPC was a significant of decreased DI ($b = -0.19$, $p = < .001$). Also, again, none of these associations were moderated by the two experimental conditions. However, while most of the associations between GPC and the internal TAM constructs were significant, in terms of the size of the associations, they were much smaller than any of three mID-specific variables (i.e., mID-SPC, mID-PPR, and mID-ANX).

For example, mID-SPC was a significant predictor of decreased PEOSU ($b = -0.30$, $p < .001$), PEOU ($b = -0.25$, $p < .001$), PU ($b = -0.29$, $p < .001$), PA ($b = -0.50$, $p < .001$), and DI ($b = -0.56$, $p < .001$) and none of these associations were moderated by the experimental conditions (see Fig. 5 for mID-SPC predicting DI in all four experimental conditions). Also, the pattern of associations was similar for mID-PPR and mID-ANX predicting the four internal TAM constructs and DI.

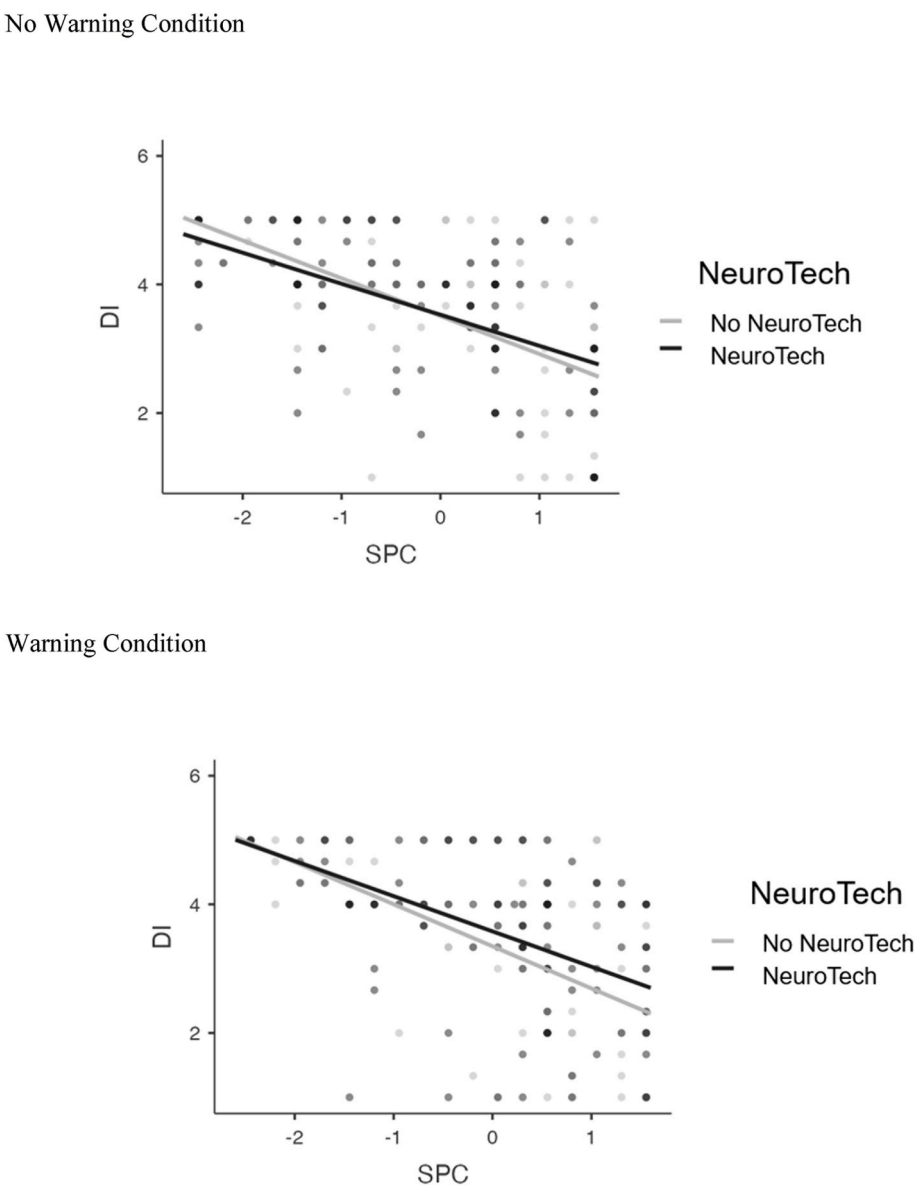


Fig. 5. Download intentions for the four conditions. *Note*. In the figure above we display the associations between SPC predicting DI in all four experimental conditions. Importantly, this negative association was no moderated by the experimental conditions: $b = -0.59$, $b = -0.48$, $b = -0.65$, and $b = -0.55$, respectively, all p's < 0.001, in the four conditions as listed above.

Finally, only three of these associations were moderated by the experimental conditions. First, the negative association between increased mID-PPR and DI was stronger in the Warning condition ($b = -0.64$, $p < .001$) compared to the No warning condition ($b = -0.47$, $p < .001$). Second, the negative association between increased mID-ANX and PA was stronger in the No NeuroTech PET condition ($b = -0.60$, $p < .001$) compared to the NeuroTech PET condition ($b = -0.41$, $p < .001$). Third, the negative association between increased mID-ANX and DI was stronger in the Warning condition ($b = -0.64$, $p < .001$) compared to the No warning condition ($b = -0.46$, $p < .001$). Though, in each of these cases, moderation is due to a stronger effect only. In sum, increases in mID-SPC, mID-PPR, or mID-ANX all lead to *moderate* decreases in PEOSU, PEOU, and PU as well as *large* decreases in PA and DI. Furthermore, these moderate and large effects occurred in all the experimental conditions.

8.2. The impact of pairing a PET with the mID

Given these regression models, we aimed to test H4, H5, and H6. First, we began by examining if there were any significant differences in the external and internal TAM constructs across the two experimental manipulations. That is, through a series of 2 × 2 factorial ANOVAs, we examined the individual main effects of the Warning and NeuroTech PET conditions as well as the interaction on the TAM constructs. Importantly, there were no significant interactions in any of the factorial ANOVAs. Thus, the effects of NeuroTech PET on the external and internal TAM constructs were consistent in both the Warning and No warning conditions. Therefore, we focused our results below on the marginal means post-hoc *t*-tests for each TAM construct in each condition.

First, we examined the main effects of the Warning condition on the ratings of the external and internal TAM constructs. There was a main effect of the Warning condition on mID-PPR (t [416] = 2.73, $p = .007$; $M_{\text{Warning}} = 3.44$; $M_{\text{No Warning}} = 3.16$; $d = 0.27$) and mID-ANX (t [416] = 2.59, $p = .010$; $M_{\text{Warning}} = 3.47$; $M_{\text{No Warning}} = 3.20$; $d = 0.25$), where those in the Warning condition reporting elevated mID-PPR and mID-ANX compared with those in the No Warning condition. There also was a marginal main effect of the Warning condition on GPC, (t [416] = 1.79, $p = .074$; $M_{\text{Warning}} = 4.29$; $M_{\text{No Warning}} = 4.18$; $d = 0.18$) and mID-SPC (t [416] = 1.70, $p = .090$; $M_{\text{Warning}} = 3.55$; $M_{\text{No Warning}} = 3.35$; $d = 0.17$), where those in the Warning condition reporting moderately elevated GPC and mID-SPC compared with those in the No Warning condition. However, there was no main effect for the Warning condition on IP (t [416] = −1.43, $p = .553$; $M_{\text{Warning}} = 3.30$; $M_{\text{No Warning}} = 3.42$; $d = -0.14$) nor SI (t [416] = 0.71, $p = .476$; $M_{\text{Warning}} = 4.03$; $M_{\text{No Warning}} = 3.96$; $d = 0.07$). Also, there was no main effect of the Warning condition on *any* of the internal TAM constructs. That is, those in the Warning condition did not differ from those in the No Warning condition on: PEOSU (t [416] = 0.57, $p = .571$; $M_{\text{Warning}} = 4.10$; $M_{\text{No Warning}} = 4.07$; $d = 0.06$), PEOU (t [416] = −0.87, $p = .571$; $M_{\text{Warning}} = 4.10$; $M_{\text{No Warning}} = 4.15$; $d = -0.08$), PU (t [416] = −0.53, $p = .571$; $M_{\text{Warning}} = 4.01$; $M_{\text{No Warning}} = 4.05$; $d = -0.05$), PA (t [416] = −1.38, $p = .168$; $M_{\text{Warning}} = 3.58$; $M_{\text{No Warning}} = 3.72$; $d = -0.13$), or DI (t [416] = −1.37, $p = .171$; $M_{\text{Warning}} = 3.40$; $M_{\text{No Warning}} = 3.56$; $d = -0.13$). Thus, reading a warning about potential privacy loss using the mID significantly increased mID-PPR as well as mID-ANX as well as moderately increase mID-specific privacy concern. However, reading about a warning of potential privacy loss had no impact on the internal TAM constructs (see Table 1).

Second, we tested H4 to examine if there were main effects of the NeuroTech PET condition on DI and the ratings of the external and internal TAM constructs. We report the marginal means, standard deviations, post-hoc *t*-tests, *p*-value, 95% confidence interval around the mean difference, and *d*-effect size for each external and internal TAM construct in Table 3. In support of H4, those in the NeuroTech PET condition ($M = 3.60$; $SD = 1.16$), compared to those in the No NeuroTech PET condition ($M = 3.36$; $SD = 1.18$), reported increased DI, F (1, 416) = 4.35, $p = .038$. Thus, pairing a mID with a NeuroTech PET significantly increased DI of the mID (see Table 2).

Table 1
Means and SD for internal TAM constructs reported separately across various demographic variables.

Demographic and TAM Constructs	PESU, *M* (*SD*)	PEU, *M* (*SD*)	PU, *M* (*SD*)	PA, *M* (*SD*)	DI, *M* (*SD*)
Gender:					
Females ($N = 223$)	4.06 $_{a}$ (.66)	4.18 $_{a}$ (.62)	4.07 $_{a}$ (.75)	3.80 $_{a}$ (1.02)	3.61 $_{a}$ (1.15)
Males ($N = 223$)	4.04 $_{a}$ (.67)	4.09 $_{a}$ (.66)	3.90 $_{b}$ (.88)	3.69 $_{a}$ (1.07)	3.55 $_{a}$ (1.19)
Age					
18–29 ($N = 85$)	4.15 $_{a}$ (.65)	4.18 $_{a}$ (.65)	3.94 $_{a}$ (.84)	3.62 $_{a}$ (1.01)	3.59 $_{a}$ (1.18)
30–45 ($N = 218$)	4.08 $_{a,b}$ (.64)	4.17 $_{a}$ (.64)	4.03 $_{a}$ (.85)	3.79 $_{a}$ (1.05)	3.63 $_{a}$ (1.19)
45+ ($N = 150$)	3.93 $_{b}$ (.70)	4.05 $_{a}$ (.64)	3.93 $_{a}$ (.77)	3.74 $_{a}$ (1.05)	3.50 $_{a}$ (1.14)
Income					
< $60,000 HHI ($N$ = 240)	4.01 $_{a}$ (.68)	4.11 $_{a}$ (.69)	3.91 $_{a}$ (.92)	3.60 $_{a}$ (1.12)	3.40 $_{a}$ (1.12)
> $60,000 HHI ($N$ = 212)	4.08 $_{a}$ (.65)	4.15 $_{a}$ (.53)	4.07 $_{b}$ (.72)	3.89 $_{b}$ (.93)	3.77 $_{b}$ (1.06)
Education					
Less than College ($N = 192$)	4.04 $_{a}$ (.68)	4.12 $_{a}$ (.69)	3.96 $_{a}$ (.88)	3.75 $_{a}$ (1.04)	3.58 $_{a}$ (1.17)
Bachelor's or more ($N = 260$)	4.05 $_{a}$ (.65)	4.14 $_{a}$ (.61)	3.99 $_{a}$ (.79)	3.73 $_{a}$ (1.05)	3.57 $_{a}$ (1.17)

Note. PEOSU = Perceived Ease of Set-Up. PEOU = Perceived Ease of Use. PU = Perceived Usability. PA = Positive Attitudes Toward mID. DI = mID Download Intentions.

Table 2
Pearson Correlations between internal TAM constructs and External TAM constructs.

External Variables	PESU	PEOU	PU	PA	DI
GPC	.03	.04	.03	−.12*	−.16**
mID-SPC	−.26**	−.26**	−.33**	−.55**	−.58**
mID-PPR	−.24**	−.22**	−.32**	−.52**	−.54**
mID-ANX	−.23**	−.25**	−.33**	−.53**	−.56**
IP	.35**	.32**	.26**	.34**	.41**
SI	.46**	.45**	.48**	.53**	.53**

Note. For the external TAM constructs: General Privacy Concern = GPC; Innovative personality = IP; Social influence = SI; mID-specific privacy concerns = mID-SPC; mID-specific perceived privacy risk = mID-PPR; mID-specific anxiety = mID-ANX. For the internal TAM constructs PESU = Perceived Ease of Set-up; PEOU = Perceived Ease of Use; PU = Perceived Usability; PA = Positive Attitudes; DI = Download Intentions.

Next, we examined the impact of the NeuroTech condition on our internal constructs of PEOSU, PEOU, PU, and PA to test H5. We found partial support for H5, such that there were no significant differences for PEOSU (F [1, 416] = 1.70, $p = .193$), PEOU (F [1, 416] = 3.20, $p = 074$), and PU (F [1, 416] = 0.85, $p = .074$); however, there was a significant main effect of pairing a NeuroTech PET (M = 3.76; SD = 1.01) compared to No NeuroTech PET (M = 3.54; SD = 1.09) on PA (F [1, 416] = 4.96, $p = .027$). Thus, participants had more positive attitudes toward the mID when it was paired with the NeuroTech PET compared to when it was not paired with the NeuroTech PET.

Finally, we examined the impact of the NeuroTech PET condition on the external constructs of GPC, mIDSPC, mID-PPR, and mID-ANX. Supporting part of H6, those in the NeuroTech PET condition compared to the No NeuroTech PET reported less mID-PPR (F [1, 416] = 7.48, $p = .007$) and mID-ANX (F [1, 416] = 6.72, $p = .010$). Thus, pairing a mID with a NeuroTech PET significantly decreased mID-PPR as well as mID-ANX. However, those in the NeuroTech PET condition did not significantly differ from those in the No NeuroTech PET condition on

Table 3
Comparing the means of the TAM constructs when the mID was and was not paired with a PET.

External TAM Constructs						
	With NeuroTech *M (SD)*	Without NeuroTech *M (SD)*	*t* (416)	*p*	95% CI $M_{Difference}$	*d*-effect size
GPC	4.19 (.75)	4.28 (.58)	−1.38	.168	[-.22, .04]	−.13
mID-SPC	3.35 (1.21)	3.55 (1.11)	−1.79	.074	[-.43, .02]	−.17
mID-PPR	3.13 (1.12)	3.46 (1.00)	−3.27	.001	[-.54, −.13]	−.32
mID-ANX	3.17 (1.12)	3.50 (.97)	−3.22	.001	[-.53, −.13]	−.31
PI	3.38 (.91)	3.34 (.90)	.50	.620	[-.13, .22]	.05
SI	3.98 (.89)	4.01 (.92)	−.32	.748	[-.20, .15]	−.03
Internal TAM Constructs						
PESU	4.14 (.63)	4.04 (.69)	1.30	.193	[-.04, .22]	.13
PEOU	4.18 (.65)	4.07 (.70)	1.79	.074	[-.01, .25]	.17
PU	4.06 (.82)	3.99 (.82)	.92	.357	[-.08, .23]	.09
PA	3.76 (1.01)	3.54 (1.09)	2.23	.027	[.03, .43]	.22
DI	3.60 (1.16)	3.99 (1.18)	2.08	.038	[.01, .46]	.20

Note. For the external TAM constructs: General Privacy Concern = GPC; Innovative Personality = IP; Social Influence = SI; mID-Specific Privacy Concerns = mID-SPC; mID-Specific Perceived Privacy Risk = mID-PPR; mID-Specific Anxiety = mID-ANX. For the internal TAM constructs PEOSU = Perceived Ease of Set-up; PEOU = Perceived Ease of Use; PU = Perceived Usefulness; PA = Positive Attitudes; DI = Download Intentions.

GPC (F [1, 416] = 1.91, p = .168) and mID-SPC (F [1, 416] = 2.89, p = 090).

8.3. Exploratory mediation models

Based on the previous results from the series of factorial ANOVAs, we explored a sequential mediation model in which the relationship between pairing the NeuroTech PET with a mID and download intentions was mediated by (1) mID-specific anxiety (mID-ANX) and mID-specific perceived privacy risk (mID-PPR), and (2) positive attitudes (PA). We tested this model using the GLM Mediation Model in JAMOVI. Please see Fig. 6 for all standardized regression coefficients.

First, the NeuroTech condition (i.e., where the privacy-enhancing technology was paired with the mID) significantly decreased mID-ANX ($\beta = -0.16$, $p < .05$) and mID-PPR ($\beta = -0.16$, $p < .05$), even after controlling for the intercorrelation between the two variables (r = 0.83, $p < .05$). Second, mID-ANX was negatively related to PA ($\beta = -0.20$, $p < .05$) and mID-PPR was negatively related to PA ($\beta = -0.34$, $p < .05$), even after controlling for the NeuroTech condition. Importantly, after controlling for mID-ANX and mID-PPR, there was no direct path from NeuroTech to PA. Third, in the regression model with mID-ANX, mID-PPR, and PA, the regression coefficients for mID-ANX and mID-PPR were not significant, whereas the regression coefficient for PA ($\beta = 0.77$, $p < .05$) was significant. Thus, the indirect paths from NeuroTech - > mID-ANX - > DI and NeuroTech - > mID-PPR - > DI were not significant (see Table 4). However, the sequential mediation path with mID-ANX as the first mediator and PA as the second mediator ($\beta = 0.06$, $SE = 0.03$, 95% CI [0.01, 0.11]) was significant. Additionally, the second sequential mediation path with mID-PPR as the first mediator and PA as the second mediator ($\beta = 0.10$, $SE = 0.04$, 95% CI [0.03, 0.17]) was also significant.

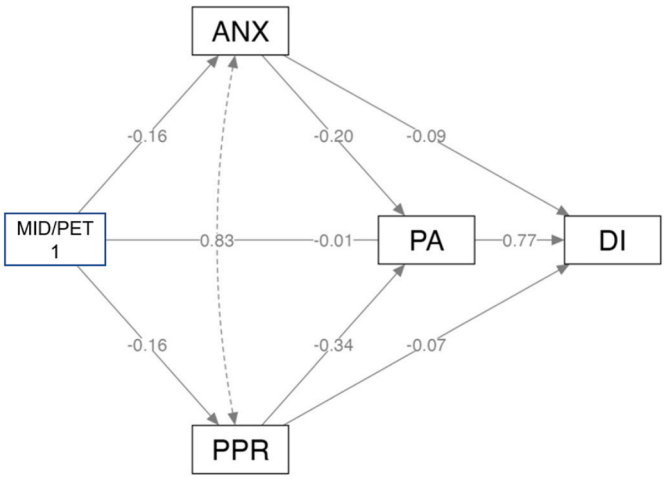


Fig. 6. Prediction of download intention for mobile identification specific constructs. *Note:* Categorical independent variables (factors) are represented by contrast indicators. For variable MID/PET1 the contrasts are: MID/PET1 = MID/PET- MID.

The results suggest that the pairing of NeuroTech PET with the mID simultaneously decreased mID-ANX and mID-PPR, which increased PA. Furthermore, it is predicted that by decreasing mID-ANX and mID-PPR, which increased PA, DI increased correspondingly. Therefore, pairing NeuroTech PETs with other technologies may increase PA (via decreased mID-ANX and mID-PPR) and ultimately increase DI.

9. Discussion

Understanding the cognitive (privacy concerns) and affective (mID anxiety) barriers to technology adoption is an important goal across many areas of research because of the extensive body of literature linking privacy concerns and technology anxiety with reduced technology adoption (Johnson et al., 2018; Lin & Kim, 2016; Liu & Tao, 2022; Zhang, Luximon, & Li, 2022; McFarland & Hamilton, 2006; Park et al., 2014). Across two studies, we examined the predictors of adoption of the mID, an app that will provide many with the power to choose what personally identifiable information to share, but may have barriers to adoption due to privacy concerns, within the framework of TAM.

In Study 1, we established the positive and negative predictors of adoption of mID. Consistent with H1 and prior research (Davis, 1989; Davis et al., 1989; Haugstvedt & Krogstie, 2012; Lin & Kim, 2016; Oyman et al., 2022; Park et al., 2014; Park et al., 2007), a user's perceptions of the ease of set up, ease of use, usefulness, and positive attitudes for the mID app strongly predict intention to use. Furthermore, consistent with H2, GPC, mID-SPC, mID-PPR, and mID-ANX were all negatively associated with DI, which also follows extensive prior research (Demoulin & Djelassi, 2016; Johnson et al., 2018; Xu et al., 2012). Finally, having an innovative personality and finding technology to be socially influential, our two individual difference variables, were also positive indicators intention to download a mID app, supporting H3 and past research (Sun & Chi, 2019). As such, we replicated the large body of TAM literature.

Additionally, our research explored a novel solution to barriers to adoption of the mID, namely through the use of a NeuroTech PET. First, and importantly, in Study 2, we found that pairing a NeuroTech PET with the mID (compared to not) led to significant increases in download intention (supporting H4), positive attitudes (partially supporting H5), mID-PPR, and mID-ANX (partially supporting H6). These results demonstrate that the NeuroTech PET is a viable solution to mID adoption barriers. Importantly, the NeuroTech PET also improves expected

Table 4
Exploratory mediation model examining the relationship between pairing the mID with the NeuroTech PET and DI.

Type	Effect	Estimate	SE	95% C·I.		β	*z*	*p*
				Lower	Upper			
Indirect	NeuroTech ⇒ PPR ⇒ DI	0.03	0.02	−0.01	0.06	0.01	1.35	0.177
	NeuroTech ⇒ ANX ⇒ DI	0.03	0.02	0	0.07	0.01	1.74	0.083
	NeuroTech ⇒ PPR ⇒ PA ⇒ DI	**0.1**	**0.04**	**0.03**	**0.17**	**0.04**	**2.65**	**0.008**
	NeuroTech ⇒ ANX ⇒ PA ⇒ DI	**0.06**	**0.03**	**0**	**0.11**	**0.02**	**2.03**	**0.042**
Component	NeuroTech ⇒ PPR	−0.34	0.1	−0.54	−0.14	−0.16	−3.28	0.001
	PPR ⇒ DI	−0.07	0.05	−0.17	0.02	−0.07	−1.48	0.139
	NeuroTech ⇒ ANX	−0.33	0.1	−0.53	−0.13	−0.16	−3.25	0.001
	ANX ⇒ DI	−0.1	0.05	−0.2	0	−0.09	−2.05	0.04
	PPR ⇒ PA	−0.34	0.07	−0.48	−0.19	−0.34	−4.57	<.001
	PA ⇒ DI	0.86	0.03	0.8	0.93	0.77	26.56	<.001
	ANX ⇒ PA	−0.2	0.07	−0.34	−0.05	−0.2	−2.62	0.009
Direct	NeuroTech ⇒ DI	−0.02	0.06	−0.13	0.1	−0.01	−0.3	0.767
Total	NeuroTech ⇒ DI	0.24	0.11	0.01	0.46	0.1	2.08	0.038

Note. mID-Specific Perceived Privacy Risk = mID-PPR; mID-Specific Anxiety = mID-ANX. PA = Positive Attitudes; DI = Download Intentions.

outcomes such as making users feel more positive towards the mID as well as decreasing feelings of perceived privacy risk and anxiety associated with the mID, which has been shown in past literature to improve intentions to use a technology (Lin & Kim, 2016; Liu & Tao, 2022; Zhang, Luximon, & Li, 2022; Johnson et al., 2018; McFarland & Hamilton, 2006; Park et al., 2014).

Based on the results of H4 – H6, we conducted an exploratory analysis to examine how the NeuroTech PET led to increased DI. Because feeling less privacy risk and anxiety with the mID should improve users' attitudes with the mID, we decided to conduct an exploratory mediation model to test this in an exploratory fashion. We found that when pairing the NeuroTech PET with the mID (compared to not), users reported less mID-related perceived privacy risk and less mID-related anxiety, which increased positive attitudes towards the mID and thus improved download intentions. However, because this was an exploratory analysis, we highly recommend this finding be replicated in future research not only with this exact design but also with a physical mID and a NeuroTech PET being paired.

9.1. Limitations and future research

There are several limitations to note. First, our study relied on slides to convey the features of both the mID and the NeuroTech PET. As such, our experiment was purely hypothetical, asking participants in our study to imagine using a mID and a NeuroTech PET. Although this experimental design is less strong than having a physical mID and NeuroTech PET paired, the results of our study still demonstrated that the NeuroTech PET led to increased download intention and positive attitudes, as well as decreases in mID-related perceived privacy risk and mID-related anxiety. However, it is important for future research to not only replicate this hypothetical research design, but also it is vital to take this experiment into the real world by physically pairing the mID with a NeuroTech PET to examine whether the results of this research can be reproduced.

Furthermore, this study is one of the first to pair technologies in order to improve intention to use a technology. As such, we cannot be sure that this same pairing model holds true for other technology beyond the pairing of the mID and NeuroTech PET. Thus, future research should use our pairing model to investigate whether pairing technology may be a viable way to improve the intention to use other new technologies.

Additionally, our sample for both Study 1 and Study 2 was recruited via Amazon's Mechanical Turk. Although this sample allowed us to gather responses from participants from a diverse background in the United States, it would be wise to replicate this research using diverse recruiting strategies such as with community samples, multiple worksite samples, or university samples to negate recruitment biases. Importantly, future research should use the TAM in experimental designs such as the one we employed. Not only was TAM fruitful in this research, but it was also helpful in recent research investigating education (Almaiah et al., 2022; Almaiah et al., 2022).

10. Implications

Because mIDs are becoming a ubiquitous form of technology to verify one's personal identity, it is important to understand the barriers to adoption. Importantly, due to the sensitive nature of the information housed on mIDs, it is important for every individual's privacy be protected in the most secure way possible. As such, across two studies, we found that concerns with privacy and anxiety with the mID are two major barriers to adoption. However, when the mID is paired with a biotechnology PET, users are more likely to use the mID and to have a more favorable view of the mID. By pairing the biotechnology PET with the mID, we were able to reduce feelings of privacy-risk, anxiety, and even increase positive attitudes towards the mID.

This research strengthens the TAM literature in a few ways. This current research is not only one of the first explore the adoption of the mID using the TAM, but this research also provides an extension of the traditional five internal TAM constructs (e.g., PEOSU, PEOU, PU, PA, and DI) by including six external cognitive and affective TAM constructs (e.g., IP, SI, ANX, GPC, mID-SPC, and mID-PPR) that have been linked to increased adoption in previous research. Importantly, our research provides a unique contribution to technology acceptance by creating a new technology acceptance framework that has never been explored before by pairing a privacy enhancing technology (NeuroTech PET) with the mID to reduce privacy concerns and anxiety and improve the technology adoption of the mID.

Furthermore, although anxiety and privacy concerns are typically strong barriers to adoption in the TAM literature (Johnson et al., 2018; Lin & Kim, 2016; Liu & Tao, 2022; Zhang, Luximon, & Li, 2022; McFarland & Hamilton, 2006; Park et al., 2014), a hypothetical biotechnology PET was able to relieve these concerns. Perhaps future research employing a real biotechnology PET may find even stronger effects compared to our hypothetical model. Second, our research employs a pairing model where we paired the mID with a biotechnology PET. Our results demonstrate that using a pairing model in the TAM literature might be a strong way to understand technology adoption. And specifically, biotechnology PETs may be a viable way to make users feel more secure with their privacy, especially when it comes to any technology that is tied to privacy concerns and anxiety.

11. Conclusion

The mID houses personal information such as one's name, date of birth, or address, which can provide benefits to the user including contactless proof of identity (like when entering a concert) and control over the personal information that is shared (such as when verifying age

at a bar). However, mIDs do not provide the level of protection that is necessary to ensure that one's personally identifiable information is properly secured from hackers or third parties. These privacy concerns may be a barrier to adoption among the greater population. As such, across two studies, we explore to use of a NeuroTech PET as a solution to the privacy concerns and mID anxiety that may be a barrier to mID adoption. Our results demonstrate that pairing a NeuroTech PET with the mID, compared to not, significantly improved download intention and positive attitudes towards the mID and led to decreased feelings of perceived privacy risk and anxiety towards the mID. In our exploratory model, we also identified that the pairing of the mID with the NeuroTech PET led to increased download intention because of reduced mID-related privacy risk and anxiety, which improved positive attitudes towards the mID. Because privacy risks and technology anxiety have been shown to be strong barriers to technology adoption (Johnson et al., 2018; Lin & Kim, 2016; Liu & Tao, 2022; Zhang, Luximon, & Li, 2022; McFarland & Hamilton, 2006; Park et al., 2014), pairing technology like the mID with a NeuroTech PET may be a suitable solution to improve inadvertent privacy flaws and anxiety with a technology and thus improve positive attitudes towards a technology to improve adoption behavior.

Author note

We have no known conflict of interest to disclose.

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.

Data availability

Data will be made available on request.

Appendix A. Definitions of Technology Terminology

What is "user authentication"?

User authentication is proving your identity on any device that can access systems or networks on the internet. The methods that we create to gain access to email, websites, or apps can include passwords, lock patterns, personal identification numbers (PINs), or physical characteristics like your face or eye. User authentication methods are designed to make sure that access to the device and the information on the device are restricted to you.

What is "mobile device authentication"?

Mobile device authentication is the verification of your identity through an authentication method for secure access. Authentication is important when using smartphones and other mobile devices because a lot of sensitive information is stored in the smartphone. Authentication verifies the identity of the user that is attempting to gain access to a device like a smartphone or a tablet. Users have to prove their identity through usernames, IDs, passwords, lock patterns, and personal identification numbers (PINs). Other methods use your fingerprint, eye, or face to make sure you are the one that is accessing your smartphone or device which is considered biometric authentication.

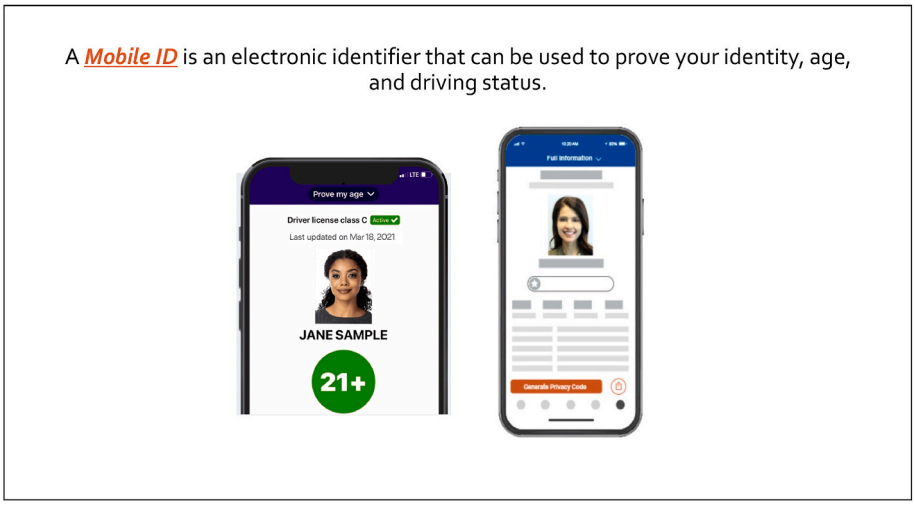
What is "biometric authentication"?

Biometric authentication uses some part of your physical characteristic that makes sure to prove your identity when you are using your phone. There are different methods of biometric authentication that include fingerprints, eye scans, or face recognition. These methods allow you to unlock your smartphone and access apps and services using your smartphone. For example, you can create your biometric authentication by setting your lock screen to only open by your fingerprint. Biometric authentication methods protect you from hackers accessing your smartphones and apps through your unique physical characteristics.

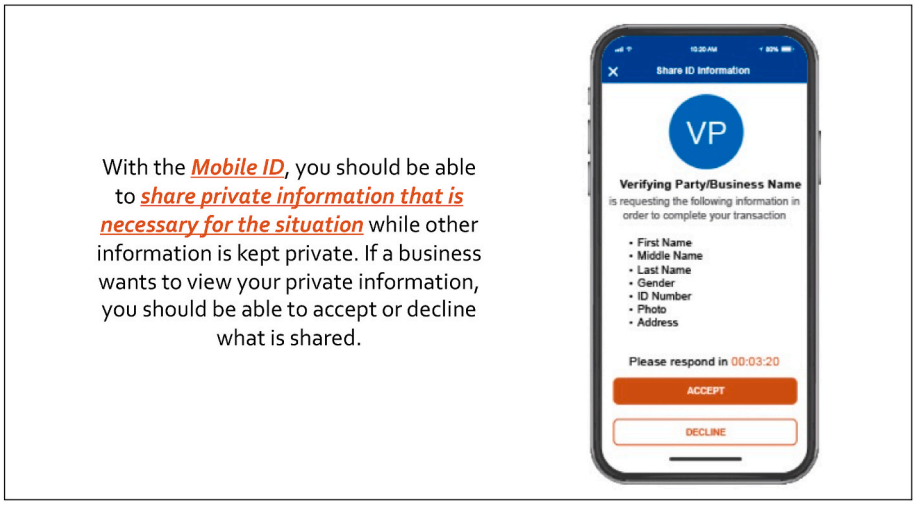
What is "data encryption"?

Your sensitive information is managed and stored online and can be vulnerable to unauthorized access and theft. Data encryption protects your sensitive information from unauthorized access, disclosure, or theft. When data is encrypted, it is unreadable by anyone that is not authorized to access this information. This means your data that is stored or transmitted would be scrambled, unreadable, and protected from unauthorized access.

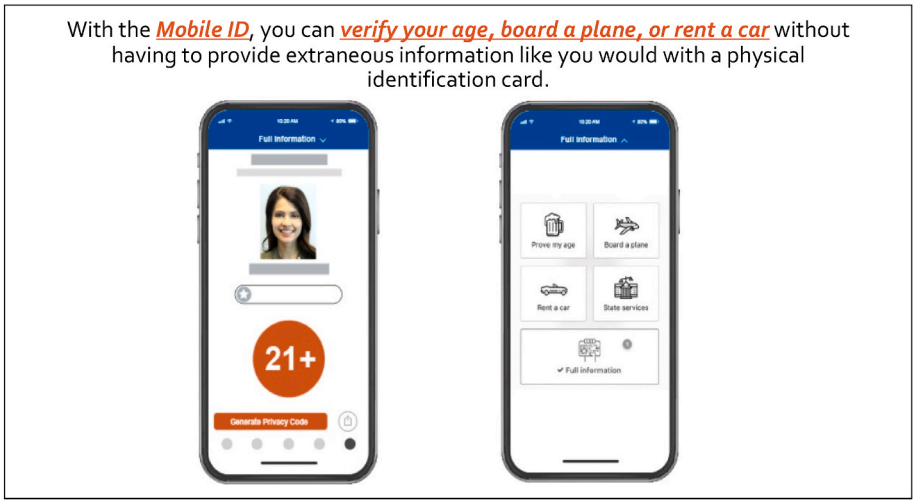
Appendix B. Mobile Identification Graphics



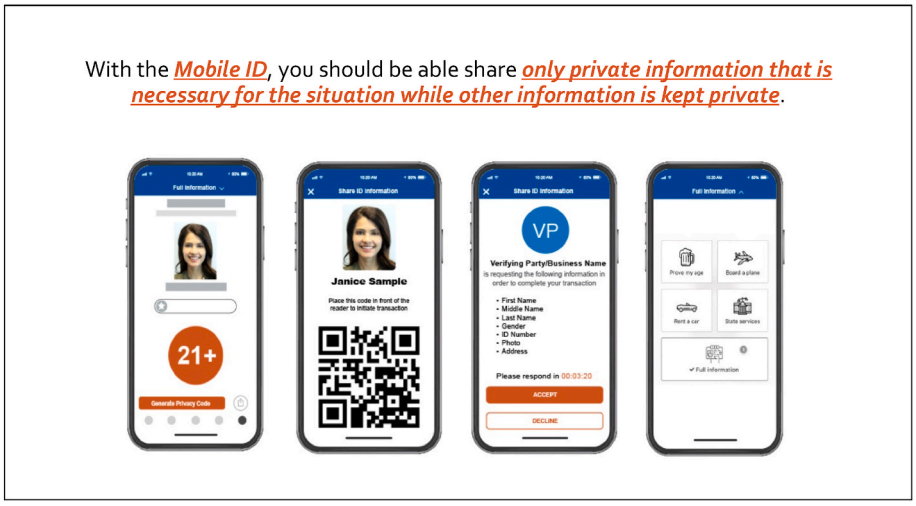
Note: Slide 1 introduces mobile identification.



Note: Slide 2 describes mobile identification information control.

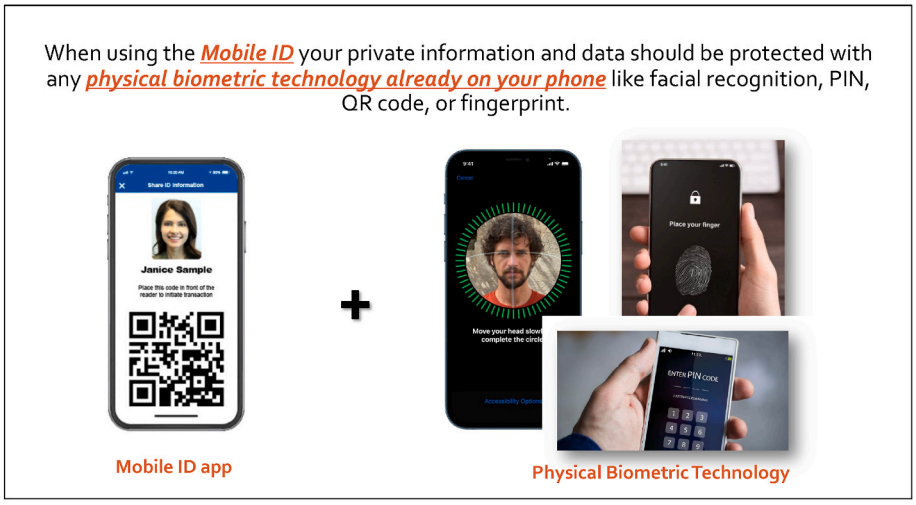


Note: Slide 3 describes mobile identification uses.



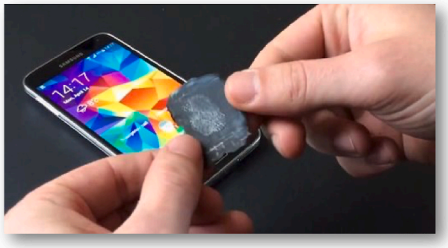
Note: Slide 4 describes mobile identification privacy.

Note: Slide 5 introduces privacy concerns about private information presented as part of the warning condition.



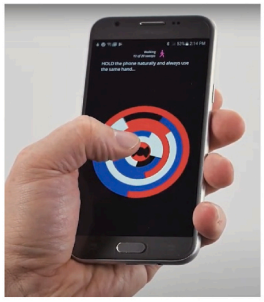
Note: Slide 6 describes the current authentication and privacy methods used by mobile identification apps.

PROBLEM #1:
However, the current *physical biometric technology* on smartphones can be *hacked, recorded, or stolen*. This lack of security leaves you *vulnerable to identity fraud* including financial, medical, or identity theft.



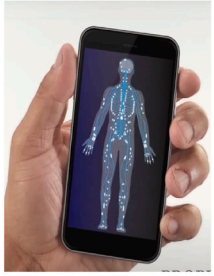
Notes: Slide 7 introduces mobile identification vulnerabilities.

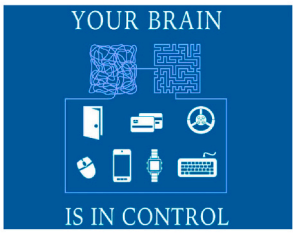
SOLUTION #1:
However, a new *physiological biometric technology*, which uses your *unique micro-vibrations or tremors in your hands* can confirm that you, the legitimate user, can securely access your private information. This technology can be added to the mobile ID at no cost to you.



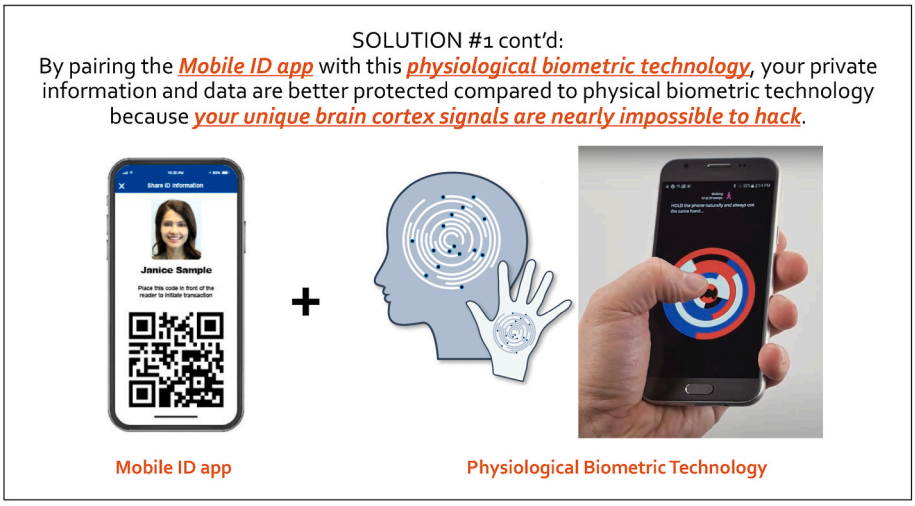
Note: Slide 8 describes a privacy enhancing technology called BioTech (NeuroTech) as a solution.

SOLUTION #1 cont'd:
This *physiological biometric technology* greatly improves your phone's security compared to existing physical biometric technology. Your micro-vibrations or tremors in your hands are *unique signals from your brain cortex that cannot be replicated* like physical biometric technology.

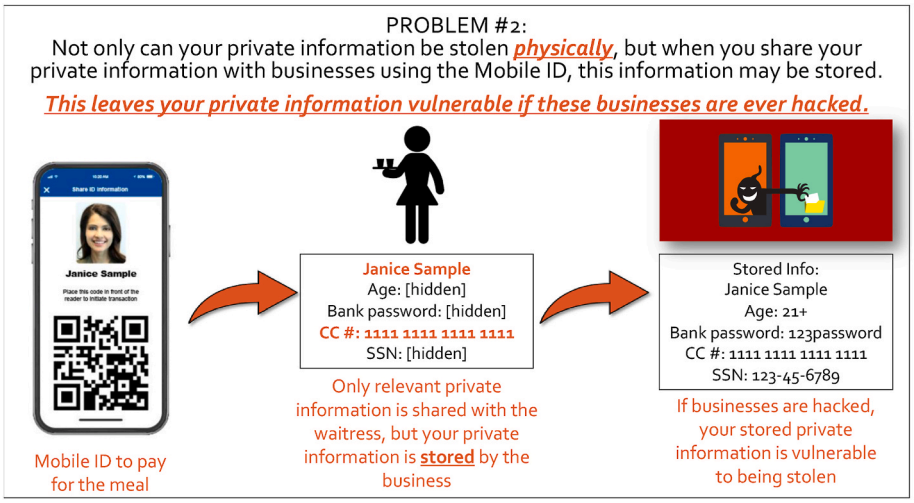




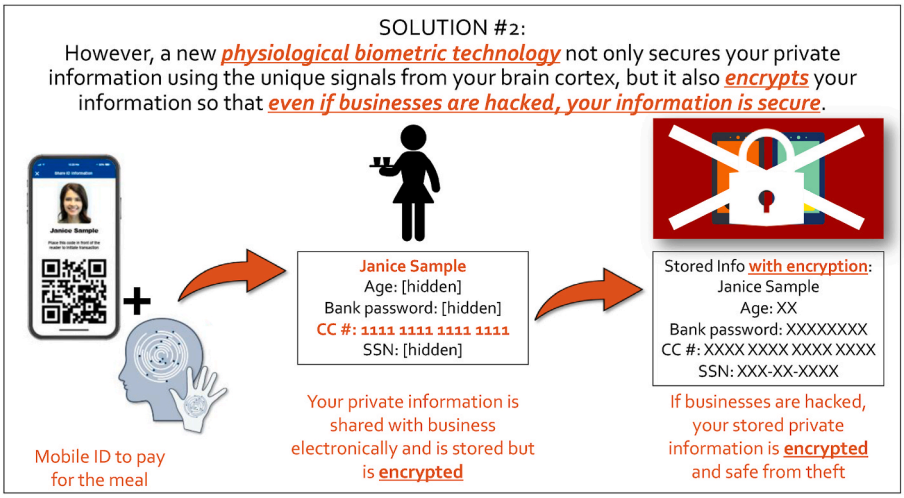
Note: Slide 9 continues to describe privacy enhancing technology.



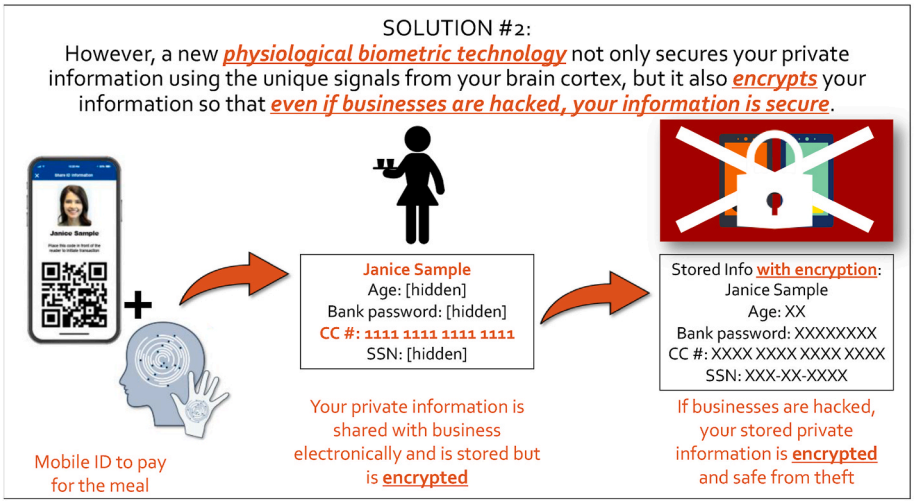
Note: Slide 10 continues to describe privacy enhancing technology.



Note: Slide 11 describes potential vulnerability of mobile identification and personal information.



Note: Slide 12 introduces BioTech (NeuroTech) the solution to mobile identification vulnerabilities.



Note: Slide 13 describes the benefits of pairing mobile identification with privacy enhancing technology.

References

Agarwal, & Prasad, J. (1999). Are individual differences germane to the acceptance of new information technologies? *Decision Sciences, 30*(2), 361–391.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211.

Akman, I., & Mishra, A. (2015). Sector diversity in green information technology practices: Technology acceptance model perspective. *Computers in Human Behavior, 49*, 477–486.

Almaiah, M. A., Alfaisal, R., Salloum, S. A., Al-Otaibi, S., Al Sawafi, O. S., Al-Maroof, R. S., … Awad, A. B. (2022). Determinants influencing the continuous intention to use digital technologies in Higher Education. *Electronics, 11*(18), 2827.

Alsaadi, I. M. (2015). Physiological biometric authentication systems, advantages, disadvantages and future development: A review. *International Journal of Scientific & Technology Research, 4*(12), 285–289.

Chang, S. E., Liu, A. Y., & Shen, W. C. (2017). User trust in social networking services: A comparison of facebook and LinkedIn. *Computers in Human Behavior, 69*, 207–217.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319–340.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982–1003.

Demoulin, N. T., & Djelassi, S. (2016). An integrated model of self-service technology (SST) usage in a retail context. *International Journal of Retail & Distribution Management, 44*(5), 540–559.

Distler, V., Lallemand, C., & Koenig, V. (2020). How acceptable is this? How user experience factors can broaden our understanding of the acceptance of privacy trade-offs. *Computers in Human Behavior, 106*, Article 106227.

Fischer-Hbner, & Berthold, S. (2017). Privacy-enhancing technologies. In *Computer and information security handbook/* (pp. 759–778). Morgan Kaufmann Publishers. https://doi.org/10.1016/B978-0-12-803843-7.00053-3.

Fishbein, M., & Ajzen, I. (1977). Belief, attitude, intention, and behavior: An introduction to theory and research. *Philosophy and Rhetoric, 10*(2).

Fox, G., Clohessy, T., van der Werff, L., Rosati, P., & Lynn, T. (2021). Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behavior, 121*, Article 106806.

Fraley, R. C., & Vazire, S. (2014). The N-pact factor: Evaluating the quality of empirical journals with respect to sample size and statistical power. *PLoS One, 9*(10), Article e109019.

Guinea, M., Stang, M., Nitsche, I., & Sax, E. (2021). Acceptance of smart automated comfort functionalities in vehicles. In *, Vol. 4. Human interaction, emerging technologies and future applications IV: Proceedings of the 4th international conference on human interaction and emerging technologies: Future applications (IHIET–AI 2021)* (pp. 331–338). Strasbourg, France: Springer International Publishing. April 28-30, 2021.

Gu, J., Xu, Y. C., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems, 94*, 19–28.

Haugstvedt, A. C., & Krogstie, J. (2012). Mobile augmented reality for cultural heritage: A technology acceptance study. In *2012 IEEE international symposium on mixed and augmented reality (ISMAR)* (pp. 247–255). IEEE.

Horne, C., & Przepiorka, W. (2021). Technology use and norm change in online privacy: Experimental evidence from vignette studies. *Information, Communication & Society, 24*(9), 1212–1228.

House Oversight and Reform; Science, Space, and Technology; Ways and Means. (2022). *Improving digital identity act 2021* (H.R. 4258).

Hsu, M. K., Wang, S. W., & Chiu, K. K. (2009). Computer attitude, statistics anxiety and self-efficacy on statistical software adoption behavior: An empirical study of online MBA learners. *Computers in Human Behavior, 25*(2), 412–420.

James, T., Pirim, T., Boswell, K., Reithel, B., & Barkhi, R. (2008). An extension of the technology acceptance model to determine the intention to use biometric devices. In *End user computing challenges and technologies: Emerging tools and applications* (pp. 57–78). IGI Global.

Johnson, A. (2020). *It's past time for the federal government to offer electronic IDs*. Information Technology & Innovation Foundation. https://itif.org/publications/2020/12/11/its-past-time-federal-government-offer-electronic-ids/.

Johnson, V. L., Kiser, A., Washington, R., & Torres, R. (2018). Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-Payment services. *Computers in Human Behavior, 79*, 111–122.

Liao, S., Lin, L., & Chen, Q. (2023). Research on the acceptance of collaborative robots for the industry 5.0 era–The mediating effect of perceived competence and the moderating effect of robot use self-efficacy. *International Journal of Industrial Ergonomics, 95*, Article 103455.

Lin, C. A., & Kim, T. (2016). Predicting user response to sponsored advertising on social media via the technology acceptance model. *Computers in Human Behavior, 64*, 710–718.

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems, 51*(3), 434–445.

Liu, K., & Tao, D. (2022). The roles of trust, personalization, loss of privacy, and anthropomorphism in public acceptance of smart healthcare services. *Computers in Human Behavior, 127*, Article 107026.

Lu, Y., Zhou, T., & Wang, B. (2009). Exploring Chinese users' acceptance of instant messaging using the theory of planned behavior, the technology acceptance model, and the flow theory. *Computers in Human Behavior, 25*(1), 29–39.

McFarland, D. J., & Hamilton, D. (2006). Adding contextual specificity to the technology acceptance model. *Computers in Human Behavior, 22*(3), 427–447.

Osatuyi, B. (2015). Is lurking an anxiety-masking strategy on social media sites? The effects of lurking and computer anxiety on explaining information privacy concern on social media platforms. *Computers in Human Behavior, 49*, 324–332.

Oyman, M., Bal, D., & Ozer, S. (2022). Extending the technology acceptance model to explain how perceived augmented reality affects consumers' perceptions. *Computers in Human Behavior, 128*, Article 107127.

Pan, & Jordan-Marsh, M. (2010). Internet use intention and adoption among Chinese older adults: From the expanded technology acceptance model perspective. *Computers in Human Behavior, 26*(5), 1111–1119.

Park, N., Lee, K. M., & Cheong, P. H. (2007). University instructors' acceptance of electronic courseware: An application of the technology acceptance model. *Journal of Computer-Mediated Communication, 13*(1), 163–186.

Park, N., Rhoads, M., Hou, J., & Lee, K. M. (2014). Understanding the acceptance of teleconferencing systems among employees: An extension of the technology acceptance model. *Computers in Human Behavior, 39*, 118–127.

Sodhro, A. H., Sennersten, C., & Ahmad, A. (2022). Towards cognitive authentication for smart healthcare applications. *Sensors, 22*(6), 2101.

Sun, & Chi, T. (2019). Investigating the adoption of apparel m-commerce in the US market. *International Journal of Clothing Science & Technology, 31*(4), 544–563. https://doi.org/10.1108/IJCST-03-2018-0038

Sun, Y., Wang, N., Shen, X. L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior, 52*, 278–292.

Thales. (2022). National ID cards: 2016 – 2022 facts and trends. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/2016-national-id-card-trends.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425–478.

Vimalkumar, M., Sharma, S. K., Singh, J. B., & Dwivedi, Y. K. (2021). 'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. *Computers in Human Behavior, 120*, Article 106763.

World Bank Group, & Global Partnership for Financial Inclusion. (2018). *G20 digital identity onboarding*.

Wu, B., & Chen, X. (2017). Continuance intention to use MOOCs: Integrating the technology acceptance model (TAM) and task technology fit (TTF) model. *Computers in Human Behavior, 67*, 221–232.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2012). Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research, 23*(4), 1342–1363.

Yuan, D., Lin, Z., & Zhuo, R. (2016). What drives consumer knowledge sharing in online travel communities?: Personal attributes or e-service factors? *Computers in Human Behavior, 63*, 68–74.

Zhang, J., Luximon, Y., & Li, Q. (2022). Seeking medical advice in mobile applications: How social cue design and privacy concerns influence trust and behavioral intention in impersonal patient–physician interactions. *Computers in Human Behavior, 130*, Article 107178.